Me Intentaron ESTAFAR con un PHISHING de Correos

chavales bienvenidos un día más a otro vídeo del Canal bueno bueno pues aquí estamos de vuelta una vez más dirás no se supone que en el anterior vídeo habías dicho que ese vídeo era el último vídeo del año Qué haces otra vez aquí porque estoy viendo tu jeta una vez más os comento rápidamente lo que Vais a ver a continuación es un extracto de un directo en Twitch que hemos hecho hoy recientemente y bueno va a estar editado todo para ir directo al grano a lo que ha pasado para poneros rápidamente en contexto yo esta mañana estaba en el salón con mi pareja estaba tocando el piano de chill cuando de pronto me llega un SMS que es este de aquí ahí lo estáis viendo aunque Bueno voy a poner un poco de zoom dice su paquete ha sido puesto en espera debido a que falta un número de calle en el paquete por favor actualiza la información de entrega y bueno el link ahí que me ponen cuidado eh efectivamente me han intentado colar un fishing a mí que soy el mejor hacker de España y del mundo y claro un hacker de semejante nivel es imposible que caiga ante un fishing no así que bueno me he propuesto me propuse por la mañana analizar un poco El dominio y ver un poco Ahí la estafa Cómo es que se la estaban montando el intento de fishing para robar mis datos que me intentaron hacer y Bueno la verdad es que estuvo bastante interesante porque esta tarde hice un directo en Twitch donde analizábamos todo paso a paso viendo por qué dominios pasábamos comoo al final del todo intentaban pillar mis datos de mi tarjeta de crédito espectacular y Bueno pillamos hasta paneles de administración de la propia web de fishing nada es un disparate va a estar bastante interesante el análisis al dominio como tal Y bueno así aprendéis también a analizar dominios ver a qué páginas estás dando tus datos y Cómo identificar ahí si es un fishing o no así que nada me despido por aquí y os dejo con el directo que hicimos de Twitch disfrutadlo Vale pues atentos la URL como tal vamos a ver qué coño es esto Bueno yo tengo por aquí el firefox y la URL supuestamente es esta link r. it f40 xh est Esto me lo voy a copiar por aquí para tenerlo a mano vamos a ver esto a dónde te lleva no Esto me llegó por SMS y supuestamente Pues lo he dicho hay un paquete en espera y tengo que proporcionar un número de calle en el paquete Bueno pues nos metemos y fijaros os lleva a correos.es que clo yo de primeras cuando vi esto dije hostia estarán usando caracteres unicodes de estos o unicodes de que la e es una e pero no es una e y demás realmente no O sea esta es la web oficial sí que es cierto que de primera lo que intenté hacer fue una Navegar Iniciar sesión eh proporcionar mis datos intentar ver si de alguna forma están enviando mis datos a por algún lado de alguna manera y estén utilizando alguna movida sofisticada y tal pero realmente no estuve interceptando desde burb Suite que ya sabéis que burb Suite es un intermediario actúa como un Proxy de forma que tú todo el tráfico de tu navegador puedes pasarlo por aquí y puedes ir viendo todas las peticiones que se tramitan y tal no bueno no vi nada raro y dije hostia qué extraño y claro curiosamente si me meto desde el móvil si yo me meto por ejemplo desde el móvil fijaros que sin embargo me lleva a esto fijaros spac correos. toop y veo otra página que desde el navegador pues no se veía bueno esto tenía pinta de que era el user ent a ver qué pasó esto pors ahora vale intercepto Bueno si tú por ejemplo esto lo envías al repeater si os fijáis de esta solicitud que nosotros enviamos pues bueno en la respuesta fijaros que hay un redirect y os redirige directamente a correos.es no entonces bueno dije hostia Y por qué desde el móvil Sí que puedo ver la página y desde mi Cali no entonces bueno como yo estoy empleando firefox y no estoy desde un móvil dije hostia estará entrando en conflicto el user agent y detectan los cabrones si estás desde móvil porque claro cuando estás desde móvil normalmente

El dominio cuando estás navegando por la página se oculta Hay a veces que cuando te metes en una página El dominio se queda como en la parte de abajo oculto y no lo ves por tanto me imagino que hay más probabilidad de que la víctima no sepa En qué dominio está navegando entonces Bueno aquí lo que había hecho simplemente fue esto vamos a dropear bueno había puesto en plan iPhone user agent que al final Esto lo puedes manipular ent Bueno me había metido en esta página y lo que vamos a intentar Es que desde el navegador nos cargue la web tal y como lo vemos desde el móvil no porque uno dirá bueno cargas esto y ya está No pues no curiosamente no hace un montón de validaciones chulas que vamos a estar investigando entonces Bueno si tú pones por aquí por ejemplo este user agent fijaros como por simplemente poner un user ent de un iPhone en vez de un 302 F le das a sent Y ahora te carga otra cosa que en este caso bueno está intentando cargar un recurso javascript que está aquí no static js.js Bueno yo en este punto lo que dije fue Vale pues para automatizar lo que es todo este proceso de que el user agent me lo cambie al mío al que me interesa lo que hice fue pasar esto por burb Suite y bueno lo cómodo de burb Suite es que tú puedes crear reglas tú lo que puedes hacer es por ejemplo el user allente es este no Supuestamente efectivamente match and replace tú esto te lo puedes copiar y le dices Bueno pues vamos a donde ponga en cuanto a cabecera de solicitud donde ponga esto pues quiero que me lo cambies a este otro user agent de forma que bueno te ahorras el tú tener que estar por cada solicitud cambiándolo que es un coñazo bueno Vamos a darle a Ok entonces Bueno lo que conseguimos con esto es que por ejemplo si yo ahora intercepto y esta misma página la recargo bueno veréis como ahora pone iPhone y yo no tengo que estar continuamente cambiándolo no entonces dije vale Ya estoy con un iPhone supuestamente a través del user ya me tiene que cargar la web No pues le das y te sigue llevando a correo y dije cómo no se supone que lo único como tal de un dispositivo móvil que se puede estar arrastrando en tal caso distinto es el user no Bueno pues me dio por curios er un poco a ver qué validaciones estaba haciendo esto porque fijaros que cuando el user agent es en este caso de un iPhone está cargando un recurso javascript no esto de aquí mira si tú te vienes por ejemplo aquí y lanzas un curl a esto https spa correos pun top creo que era No pues bueno es super extraño vamos a decirle bat menos l Java para verlo un poco mejor Bueno fijaros aquí está creando como un una especie de html sobre la marcha pero la cosa es que esto está cargando tres recursos javascript que es axios.js jquery ui.js y resource red config.js no bueno estos dos realmente dan un poco igual No necesitamos ni inspeccionarlo siquiera ya os adelanto que no hay nada interesante aquí la chicha está en este archivo que fijaros si aplicamos un curl a ese otro archivo vamos a ver qué es lo que contiene vamos a esto ponerlo ahí Bueno fijaros aquí se ve no te dice Bueno un condicional si Navigator webdriver es false lo que va a hacer es entrar aquí dentro y fijaros aquí que hay unas unas validaciones que se aplican en plan por ejemplo esto Supongo que bueno Google Bot image Google Bot news Aquí está validando el user agent para detectar que no seas en plan un Bot No pues bueno si utilizas alguno de estos user ents fijaros lo que hace es que te redirige a correos.es sin embargo Claro mi user agent ya supuestamente es iPhone que de hecho es lo que tiene por aquí contemplado dice De lo contrario si Android webos iPhone iPod o BlackBerry que son distintos tipos de dispositivos No pues lo tienes como user agent entonces lo que quiero que me hagas es que me cargues el recurso Data Jason por tanto algo me hizo pensar que esto es lo que no estaba aplicando entonces bueno intenté hacer un montón de cosas tanto desde a nivel de la consola de desarrollador de el navegador hasta desde burb Suite intenté hacer un par de cosas pero no exitosas y luego pensé en Por qué no hacer que mi equipo actuara como un Proxy de forma que ahora yo manejo todos estos recursos y los

altero Entonces por ejemplo aquí lo que había llegado a hacer fue esto está interesante para que si tenéis algún ejemplo del estilo Pues que sepáis cómo operar mir a mí lo que se me ocurrió por ejemplo fue aquí la idea es que cuando tramitamos esta solicitud el servidor está intentando cargar este recurso no static js es.js que esto reside en el propio servidor en la máquina víctima no bueno la máquina víctima en la máquina que es la que está hosteando el fishing la propia web entonces dije Bueno esto de aquí lo interesante sería como tal este recurso alterarlo para quitar esta validación quitar esta validación quitar esta validación si tal también y ya directamente cargar el data.to json y todo esto no entonces claro para eso tendría que cargar tu recurso alterado entonces Bueno a mí lo que se me ocurrió hacer fue este recurso es.js Bueno si tú por ejemplo haces esto vamos a echarle un ojo otra vez a este recurso esto de aquí bueno Esto mismo me lo traje a local es decir esto por aquí vamos a meterlo como es.js y bueno como lo está trayendo de un directorio static js pues lo que dije fue Vale pues voy a crearme los directorios static js y meto este recurso dentro de static js no qué consigues con esto Bueno si yo por ejemplo me montara un servidor Http con python por el puerto 8 8000 que es por defecto por donde te lo monta pues bueno si tú por ejemplo te vienes por aquí esto Qué es el body de la respuesta del servidor no tú en vez de cargarlo en local del servidor puedes cargar tu propio recurso en local Host de forma que una prueba que podríamos hacer es esta tú esto te lo puedes copiar y en el match and replace este pues creas una nueva regla y le dices Oye en la respuesta en la parte del cuerpo lo que tenga esto quiero que me lo conviertas a y aquí le dices http local Host por el puerto 8 1000 no en plan quiero que me cargues ahora mi recurso es.js Bueno tú le das a Ok de forma que ya creas esta regla y bueno para que veáis cómo se ve esto si yo por ejemplo esto ahora lo intercepto https vamos a decirle spac correos. top creo que era no vamos a decirle enter vale vamos a interceptar la respuesta de esta solicitud Vamos a darle a Forward y fijaros que en la respuesta ya me está intentando o me va a intentar cargar mi recurso es.js no Bueno si tú te vienes por aquí no hay ninguna solicitud y le das a si le das a Forward Ya por aquí veis que hay un una solicitud que se ha tramitado pero claro ya como tal nos ha redirigido a correos.es porque no estamos cumpliendo la validación no entonces bueno por qué estoy haciendo esto porque tú ahora tienes control local en el sentido de que bueno si tú por ejemplo ahora echas un ojo a este recurso este recurso que es el que nos interesa alterar Pues bueno como ahora lo está cargando de nuestro recurso es.js lo que dije es Oye tú ahora me vas a cargar estos dos recursos el axios y el jquery de la web que es el fishing todo sin cambiar pero este como lo voy a alterar en local quiero que me lo cargues en local en mi propio equipo no entonces bueno Esto vamos a guardarlo y vamos a tener que descargarnos el resource Red config.js entonces bueno como esto está también en static js tú lo que puedes hacer es que este recurso te lo puedes traer aquí como resource red config.js y Bueno yo lo que hice fue Quitar todas las validaciones en plan mandarlas a tomar por culo esto fuera esto fuera est fuera la validación que compruebo a través del condicional si soy un Bot o no también fuera todo esto fuera todo esto fuera y en MZ de els bueno directamente metemos esta condición que de hecho Eh bueno Esto también Fuera fuera no quiero que me redirija a correos.es esto nada entonces bueno esta llave que está cerrando desde este condicional yo lo que hice fue esto quitarlo y esto también quitarlo y bueno todo esto pues meterlo acá de forma que claro si ahora me cargas este recurso resourceconfig js directamente me vas a cargar esto de aquí Que bueno aquí ya está cargando el data.to Jason del servidor que como existe no lo cambio a mi data.to Jason local no hace falta entonces bueno dejé esto así y ahora lo que hice fue que me fui para acá entonces bueno el servidor no estaba montado me monto esto y bueno ya como tenemos la regla está creada para

que tire de nuestro recurso es.js y ahora nuestro recurso es.js pues carga nuestro recurso resource r. config La idea es que si tú ahora por ejemplo vamos a quitar el intercept esto Drop fuera Bueno si tú Aquí pones no sé si estar cacheado spac correos. top vale fijaros Ahí ha intentado Bueno ahí está ojo ojo eh Bueno pues esto es lo que yo veía en el móvil o sea que fijaros la mini validación que estaban aplicando por detrás eso es lo cómodo que tú en local te puedes traer ciertos recursos para que te los tuyos y medio alterar el código javascript para que las validaciones que no quieras que se acontezcan pues las quites las omitas y ya vayas directamente donde te interesa no bueno fijaros los cabrones este SMS que me había llegado ponía localizador de envío bueno fijaros que El dominio nada que ver pion correos. top pero muy top Supongo que por eso El dominio es top el hecho de que desde el móvil te cargue la web y desde un dispositivo que no sea un móvil no eso está interesante y bueno programa Tu entrega no te sale este identificador que no es válido y nada se ha notificado al destinatario que complete la dirección para volver a realizar la entrega no un bulto el que tengo aquí abajo preadmisión en camino 13 de diciembre est a a 13 de diciembre Bueno este dominio el spac correos. top Me parece que lo registraron creo que ayer fijaros que eso la fecha de creación fue bueno el 17 de noviembre o sea que desde el mes pasado que están ahí tensando la potente y a saber a saber todo lo que habrán recopilado vamos a ver hasta dónde te lleva Esto bueno Qué pasa que en este punto dije Vale pues programa Tu entrega pincho y me lleva a correo y dije cómo que han colado aquí que no estoy viendo pero no es porque se aplica otra validación más una que no tenemos contemplada si tú por ejemplo Ah esto lo intercept y le das a programa Tu entrega fijaros que bueno si miramos la respuesta de esta solicitud vamos a interceptar la respuesta Forward fijaros que ahora está cargando otro recurso que es static js y en MZ de es.js es2 de segunda fase de validación pun js no Bueno qué hice lo mismo me lo traje a local es decir aquí mismo en static js o bueno me traje a local el recurso este que vamos a echarle un ojo a ver cómo se ve s 2.js es la misma mierda no cambia nada de hecho creo te carga un axio un jquery y un resource Red config que es el que vamos a alterar para que no nos aplique pues toda la validación no Entonces nada lo que hice fue que esto mismo me lo traje aquí como s 2.js vamos a ver si le lo hemos descargado bien Ahí está y nada Pues ahora este recurso lo alteramos para que en vez de que nos cargue el propio resource red config del servidor que es el del fishing pues que nos cargue el nuestro no otra vez local Host Puerto 8000 y ahí está entonces Bueno qué conseguimos con esto Pues bueno como el server ya está montado H si tú ahora Bueno vamos a tener que hacer esto otra vez esto te lo copias y tienes que volver a crear por aquí una minir regla at y bueno esto sería del cuerpo de la respuesta en un principio y nada esto Pues cuando salga quiero que me lo transformes a http localhost por el puerto 8000 no Bueno le das a Ok y con esto hecho si tú ahora por ejemplo vuelves a recargar esta página vale Ahí te sale No localizador de envío bueno Estos son datos que tú tienes que proporcionar claro a spac correos. toop Entonces nada le dices por ejemplo si hombre para que me dox todo esto llegará al atacante me imagino qué era esto primer apellido seens setena indica una dirección si hombre para que me dox código postal 38310 esto es localidad eh andorra provincia Aragón Bueno cualquier cosa es que Vais a ver no tiene ni que tener sentido porque aquí te están recopilando ya datos vamos a ver a dónde se envía esto y demás bueno email test @test comom teléfono 1 2 3 45 6 789 o sea vamos a ver cuál es el objetivo no del atacante en plan A dónde quiere llegar con todo esto Si tú esto te lo intercept ahora pues bueno Vamos a darle a continuar Entonces fijaros estás enviando una petición por post donde envías todo estos datos a quién bueno para empezar a spac correos. toop que no es la web oficial Bueno tú le das a dejas que esto fluya realmente pagar con tarjeta espac correos. toop A dónde vas

cabrón estás tratando con el mejor hacker de España y del mundo Bueno qué voy a pagar para el reenvío la oficina de Correos cobrará algunas tarifas de servicios y te meten ahí 80 centimos potentes bueno tarjeta yo aquí había utilizado una de estas de tarjeta online generator vale esta Mira nosotros por ejemplo habíamos probado esto es esta tarjeta que no tiene dinero no no tiene nada vamos a copiarnos esto Bueno yo había proporcionado esto caducidad Pues bueno pones la fecha de caducidad y nada el número este te lo inventas 318 por ejemplo vamos a interceptar esto para ver a dónde estás enviando tus datos de tarjeta de crédito cvv caducidad y todo pagar Bueno fijaros en esto eh admin 666 get jy CD ya si una ruta del servidor pone get no sé qué cart Ya huele mal eso eh Nada forw forw bueno fijaros estáis emitiendo una petición por post a spa correo pun top donde le estáis dando al Señor atacante pues esto no el número de tarjeta tip code bueno Card date el cvv O sea que la idea es que te va a robar le estás dando todo al atacante alguien que proporcione por ejemplo sus datos aquí en esta mierda el atacante te va a recopilar todo eh o sea el cvv directamente ya puede utilizar tu tarjeta por ahí normalmente dependiendo de compras que se hagan si son muy grandes te debería de llegar un SMS para confirmar la operación o por ejemplo hasta con compras pequeñas en comercios electrónicos y tal a mí me salta un aviso desde mi entidad bancaria para confirmar la operación con mi cara pero igual dependiendo del banco que emplees pues no tienes esta validación Así que cuidado eh fijaros los cabrones lo que hacen Esto está interesante comprueban hacen una pequeña comprobatoria en look up.bet de este número que es la tarjeta a través de una solicitud de tipo options Bueno de hecho aquí la víctima lo que vees esto no en plan Oye estamos verificando tu información por favor pacientemente espera 5 minutos bueno los cojones aquí ya te han robado todo entonces bueno si aquí por ejemplo ponemos este dominio vamos a ver esto qué demonios es y bueno fijaros Esto es como un pequeño checker un pequeño validador te ponen estos números de ejemplo Pero bueno si tú por ejemplo le pasas estos cuatro primeros números que son como para identificar la entidad me parece si tú por ejemplo pones esto fijaros que ella pone masterc deid entonces claro Qué pasa que se supone que es una tarjeta mastercard todo correcto Bueno tú dejas que esto fluya vamos a dejar que fluya a ver cómo me roban los datos y te pone por favor pague con mastercard y es una tarjeta mastercar Bueno te va a salir siempre esto es porque ya ellos acaban de recopilar la info y te han robado todo y bueno Estaba intentando una cosa también porque aquí si os fijáis de las solicitudes que habíamos visto se tramitan ciertas peticiones a esto a admin 666 get jy Card me dio por Us mear a ver esto qué coño es vamos a ponerlo aquí Bueno Tenemos que pasar por burb suit para ver todo esto porque de lo contrario no lo vamos a ver Bueno Este es el paso final Aquí no hay nada más aquí ya cualquier cosa que hagas bueno por lo menos te dan la opción de Oye me he equivocado limpio mis datos y los vuelvo a proporcionar no por lo menos son considerados Pero bueno te metes aquí y bueno te figura esto esto raro pero aquí sí que si pones admin 666 vamos a verlo en oscuro a ver esto esto creo que era en plan que te comas un mojón que la contraseña es incorrecta o algo de esto a ver dipel el nombre de usuario o la contraseña son incorrectos bueno esto tiene que ser un disparate aquí el atacante que tendrá las credenciales válidas ahí tienes que tener todos los datos recopilados tiene que ser algo tipo número de tarjeta cvv nombre direc es que todo todo lo que hayas proporcionado pues tienen que tenerlo Por aquí todo dentro administrado eh es un scam es todo para robarte los datos y que normalmente correos no envía un enlace acotado con un acortador de URL de estos y demás Así que este vídeo si lo podéis recomendar a muerte en YouTube se agradece para evitar que campañas tanto de correos como de otras entidades porque correos no es la única con la que hacen estas mierdas Pues que tengan

cuidadito y a ver si de esta forma pues tenemos un poco más de nivel de seguridad mínimo para que no nos roben los datos vamos y nada farlopa un grande Oh