73. Qatar y URLscan.io

Qatar la sede del mundial de fútbol que está a punto de comenzar Está rodeada de escándalos que tocan de cerca nuestro tema favorito el hacking es un ataque de cero clic no es un ataque de phishing no es un fallo en la forma en la que herramientas automáticas de tipo short de gestión de incidentes pueden exponer información confidencial de los usuarios que protegen al enviar urls para su análisis a urlscam.io con un episodio un tanto delicado por la naturaleza de Su contenido os damos la bienvenida a tierra de hackers comenzamos Hola hola y bienvenidos a tierra de hackers tu noticiero de ciberseguridad hecho podcast hoy es el 10 de noviembre de 2022 este es el episodio número 73 yo soy Martín vigo y está conmigo un poco más lejos de lo ya que me encuentro en albacete de conferencias pero siempre cerca de mi corazón mi estimado Alexis porros Hola Alexis qué tal ese sí el otro en el otro lado del Charco básicamente echando echando de menos la conferencia en la que estás y ver a nuestros oyentes en persona y las pegatinas que nos encanta dar no y estar un ratillo contigo también así que nada para la próxima y a todos vosotros como siempre agradeceros primero de todo que os acerquéis a ver a Martín y que le digáis Hola que nos encanta eso y también que nos digáis de forma virtual y que nos sigáis en todas las redes sociales que ya sabéis que estamos en Twitter Instagram y Facebook con el handel@tierra de hackers linkedin YouTube y Twitch como tierra de hackers los correos electrónicos no los podéis enviar a podcast@ tierra de hackers.com en discord Pues estamos podéis Acceder al servidor de discord que tenemos en tierra de hackers.com/discord y bueno lo dicho que os suscribáis que nos sigáis nos comentéis los episodios los las noticias cualquier sugerencia es bienvenida y finalmente como siempre agradecer vuestro apoyo a la pregunta del episodio que publicamos junto con cada episodio en Twitter y en el episodio anterior fue la siguiente temes ataques Hollywood yenses con drones contra redes wi-fi de tu casa o empresa teníamos cuatro respuestas en la más votada con un 37%, no muy sofisticado aún 27%, no todavía es caro 21%, sí Hardware barato 15% si fácil automatización así que tenemos vemos que más de un tercio no no lo ven no lo ven bueno Incluso un poquito más de la mitad no lo ven como un riesgo por el que preocuparse Aunque igual lo vemos en las películas como decimos siempre estamos abiertos a proporcionar ideas de guión para películas hollywoodienses sí deberíamos hacer una consultora y de ese tema Pues sí como decías tú la verdad primer día de navaja negra de esta conferencia chulísima de hecho no solo he podido conocer oyentes que alguno incluso me reconoció por la voz mañana ya iré con la camiseta pero la verdad pues a una sensación chulísima y además estuve también con las con las chicas de securitas que son otras divulgadoras en temas de ciberseguridad que tiene un canal de Twitch muy guapo y joder lo que es juntarnos con gente que se dedica a lo mismo que nosotros pues Mola Mola muchísimo Así que que muy Guay Muy bueno muy bueno iba a decir no estamos en Halloween ya pero da escalofríos no tanta tanta concentración de talento por ahí sí sí en albacete hace un frío de pelotas y nada como siempre darle las gracias a nuestros mecenas de patreon Gracias por vuestro apoyo esta semana en concreto a elfrit y a mansioni ellos dos se acaban de unir a apoyarnos económicamente en patreon y es esencial Muchísimas gracias como siempre y podéis hacer lo mismo si podéis patreon.com/tierra de hackers también dar las gracias a Mónaco ya sabéis una empresa que comparte los mismos valores que tierra de hackers hacer la seguridad más accesible y transparente nosotros a través de un podcast y morata a través de una herramienta de gestión y visualización de telemetría de datos de seguridad una empresa fundada

en silicon Valley y que está buscando muchos ingenieros sobre todo con algo de experiencia en seguridad para ayudarles a construir y hacer realidad su misión lo mejor de todo es que está contratando en todo el mundo y en rebotó así que ya sabéis monad.com y lo podéis escribir a tierra de hackers @monat.com Por cierto me escucho con un montón de eco y Y seguramente quedará así en la grabación pero es porque estoy en una sala de un airbnb en el que me estoy quedando aquí en albacete Así que no estoy en la sitio habitual donde suelo grabar que tiene lo tengo un poquito más preparado así que ya pido disculpas por si la calidad del sonido de mi lado es un poquito pobre esta vez esperemos que no sea demasiado mala y nada saltamos ya a la noticia Y es que como muchos futboleros habrán está a punto de empezar el mundial de fútbol de 2022 y el lugar elegido fue el país de Qatar desde que se eligió Qatar han sido muchos los que han hablado en contra de este país Digamos como lugar para celebrar el mundial las razones son la falta de democracia en ese país y las leyes estrictas sobre todo Comparado Pues con países europeos y de América no esto es especialmente cierto en lo que se refiere a la comunidad lgtb Qatar es un país musulmán y entre otras cosas que he visto no se permiten Pues los besos en público las mujeres no pueden maquillarse excesivamente o no pueden llevar escote y en general pues la vestimenta está también muy restringida hago este esta breve intro para dar contexto Pero me quedo ahí porque no quiero que suene demasiado a politiqueo tema religioso que no no estamos aquí para eso es simplemente dar contexto porque es muy relevante pues para esta noticia de hecho dos noticias porque me parecía interesante con la llegada del mundial centrarme en sucesos relacionados con la ciberseguridad que hayan pasado en ese país y vaya si he encontrado material diré que en este episodio hablaré de abusos y otras situaciones que pueden herir sensibilidades Así que si eres menor O prefieres no escuchar este tipo de cosas puedes saltarte este episodio el problema con la elección de Qatar no estás solo en el hecho de que se ha elegido un país opresivo para un evento deportivo mundial sino también por los escándalos de compra de votos que hubo durante la lección en 2010 muchos quizás no se acuerden pero el país elige por sorteo y había varios candidatos además de Qatar ha habido incluso juicios por sobornos por parte del gobierno de Qatar a miembros de la FIFA con derecho a voto esto también tendrá relevancia en la noticia ya que la semana pasada el buró de periodismo de investigación publicaba un extenso artículo sobre las casos de hacking a miembros de países europeos críticos con Qatar por parte del gobierno de ese país tutorial junto con otra llamada Sunday Times han conseguido acceso a la base de datos de una empresa India quien en realidad se dedica a labores de hackford ayer o bueno contrátame para hackear de manera ilegal esta empresa que llamaremos a partir de ahora organización criminal operaba bajo las órdenes de investigadores privados que a su vez eran contratados por entre otros el gobierno de Qatar esta organización opera desde gurugram en India y esté liderada por adiya Jane adiya camufla los servicios de la organización como una empresa normal de ciberseguridad y de hecho es una especie de celebridad en su país que frecuentemente pues ya aparece en televisión opiniones sobre temas relacionados con la ciberseguridad le invitan a telediarios y todo esto pues estos medios de comunicación se hicieron pasar por potenciales clientes después de viajar a India para conseguir más información de esta empresa y en concreto de su fundadora dicha mientras este medio de comunicación que publica esta investigación negociaba con él pues como cliente no grabaron las conversaciones y en estas conversaciones a dicha evidentemente quería vender los servicios pues comentaba que actualmente estaba colaborando en proyectos relacionados con la FIFA y los equipos que organizan el mundial de Qatar le tiraron más de la lengua y comentó que consiguió acceder a los buzones de correo

electrónico de perfiles de individuos muy importantes de la FIFA y que viven en Gran Bretaña Esto fue Según dice él esponsorizado por su cliente en un país del Golfo Pérsico Pues bueno este la gente los periodistas que iban disfrazados digamos de posibles clientes volvieron a seguir presionando bajo el pretexto de querer comprar más pero querer saber más las capacidades y acabó admitiendo que el cliente del Golfo Pérsico en realidad era el gobierno de Qatar pero que en realidad a él le contrató un investigador privado de Suiza llamado Jonas Rey hago un paréntesis aquí para recordaros que esta metodología ya la hemos visto en otros episodios de tierra de hackers utilizar como pantalla un investigador privado que luego es el que se encarga de contratar a servicios ilegales así el cliente no tiene digamos conocimiento No sobre el papel ni responsabilidad teóricamente Ya que él solo contrató un investigador privado ya lo que haga el investigador privado para conseguir el material que él está pidiendo ya es cosa del investigador privado Pero bueno entre las declaraciones de adicha y que tenían acceso a la base de datos de la empresa como mencionaba al principio de la noticia este medio confirmó que otros siete clientes serán también investigadores privados pero del Reino Unido de hecho el Metropolitan police uno de los cuerpos de seguridad del estado de la ciudad de Londres contrató los servicios de adiya y le dio hasta 40 objetivos diferentes a los que hackear para acceder a su correo electrónico esto el Metropolitan police pero volviendo al investigador privado suizo en realidad este trabajaba a su vez para el Billie jeans global business intelligents una empresa Privada de inteligencia Suiza cuyo fundador es Nick day un ex oficial del del mi5 que el m5 es la agencia de inteligencia británica el equivalente a la Cia en Estados Unidos básicamente acorde a documentos jurídicos por una denuncia que hubo y por tanto son documentos públicos Billie jeans global fue contratada para trabajar en un proyecto relacionado con la organización del mundial en Qatar Pues bien el investigador privado contrató los servicios de la organización criminal India para hackear los correos electrónicos de gente crítica con la elección de Qatar como sede del mundial es decir el proyecto de The Legends global relacionado con el mundial eran realidad conseguir acceso a los correos electrónicos de gente crítica con el país llaves de hecho entre los objetivos estaba por ejemplo Jonathan calbert que es el editor del Sunday Times que es parte de hecho de esta investigación y que era conocido por sus numerosos artículos exponiendo los casos de corrupción de la FIFA en concreto le hackearon días antes de publicar una noticia sobre un soborno de 100 millones de dólares que ofreció el gobierno de Qatar a la FIFA para ser elegido en la propia base de datos filtrada hay una columna con observaciones que dice textualmente hackeo completado respecto a esta a esta persona Jonathan calbert otro objetivo fue el famoso ex futbolista platini que tenía derecho a votos sobre la sede del mundial si bien platini había sido uno de los miembros que públicamente apoyaba la celebración del mundial en Qatar había rumores de que había sido presionado en una comida con el presidente de Francia en aquella época Nicolás sarkozy y el príncipe de Qatar en aquella época que ahora Rey Jake también Bing hamad altani que Bueno aquí me ha costado el nombre fue hackeado días antes de votar y de hecho platini fue contactado por el porqué nacional financiera El pnf que es una unidad francesa que lucha contra los fraudes económicos estos le contactaron por sospechas de corrupción en torno a su participación en las votaciones para el mundial Parece ser que la investigación del pnf reveló que captar estaba ansiosa por saber qué declaraciones iba platini en torno a lo que iba a votar Supongo que para saber si le tenía que seguir presionando no para que votase por ellos por cierto que quizá no lo dije de la manera en la que los indios hackeaban las cuentas de correo era puro fishing específicamente he encontrado que mandaban correos haciéndose pasar por redes sociales como

Twitter engañando a estas personalidades a resetear su contraseña y por tanto en realidad entregándosela a la organización criminal fishing de manual pero que sigue siendo tan efectivo que se usa los más altos niveles como podéis comprobar hubo más Víctimas de estos hackeos y que también eran críticas con catar casualmente no ganen no se y b que escribió un reporte cubriendo la corrupción en Qatar no solo fue hackeado él sino también su abogado o también Jean pilipín periodista del medio mediapad que fue hackeada días después de publicar un artículo sobre la investigación judicial que estaba sucediendo en torno a sobornos para la elección de Qatar en el mundial os dejo un link a la investigación en las notas del episodio para que podáis seguir indagando pero como os comentaba Esta no es la única noticia reciente que puede encontrar respecto a Qatar y el mundo del hacking me encontré otra muy chunga y relacionada con las estrictas leyes contra el colectivo lgtb que os comentaba al principio la semana pasada también se publicaba un artículo cubriendo los abusos sexuales maltratos y detenciones ilegales a personas homosexuales en Qatar todo esto que acabo de decir por parte de una entidad gubernamental pero es que además lo hacían engañándoles con cuentas falsas en aplicaciones de citas paracidas a tinder en esta publicación entrevistan a Alí un filipino que voló a acatar para trabajar allí y que es un hombre gay y como pues cualquier otra persona decidió utilizar una aplicación de citas para conocer a otras personas un día le contactó a él un hombre que le invitó a ir a su hotel y le ofreció a mayores pues unos 100 euros No aparte de para evidentemente conocer si tener relaciones sexuales allí allí decidió aceptar y se dirigió a la dirección que era en este hotel Cuando entró en la habitación le estaban esperando seis hombres según explican esta entrevista estos seis hombres eran agentes de la policía de Qatar que lo primero que hicieron según relata Lee fue lanzarlo contra la cama y violarlo lo hicieron uno tras otro mientras el comenta que uno de ellos simplemente miraba y se reía cuenta Lee que cuando terminaron le registraron la mochila que traía mientras le decían que esto que había hecho la prostitución y que además también era homosexual comenta que mientras lloraba de hecho unos de ellos lo abofeteó y le dijo que que se callase O sea que no solo la habían violado sino que lo estaban maltratando físicamente no pero es que no termina aquí cuenta como al cabo de unas horas llegó otra víctima en este caso un hombre vietnamita que entró en la misma habitación y que también sufrió los mismos abusos Y ambos fueron detenidos y llevados a una celda donde les interrogaron Coméntale que sacaron fotos de las conversaciones de la aplicación de citas en su móvil como prueba de prostitución y homosexualidad cosas ilegales en Qatar le retuvieron dos días y luego lo deportaron en el medio que cubre esta noticia entrevistan al único hombre abiertamente gay de Qatar que por supuesto ya no vive en el país vive en San Francisco ya que está exiliado comenta que son cientos los ciudadanos de la comunidad lgtb que le escriben semanalmente y le cuentan los abusos que sufren por parte de las autoridades de hecho Mohamed que es como se llama trabaja directamente con Human Rights watch la organización sin ánimo de lucro que vigila y denuncia abusos contra los Derechos Humanos muhammed cuenta que los policías detrás de estos abusos pertenecen al proventix Security department o departamento de seguridad preventiva de Qatar y que técnicamente ni siquiera Son policías sino los describe como un equipo de seguridad Nacional del gobierno o en otras palabras como una especie de mafia contratada por el propio gobierno que puede operar a sus anchas comenta que su su modo operandi es precisamente ese engatusar a las víctimas a través de perfiles falsos en aplicaciones de citas para conseguir pruebas y traerlas Pues a un hotel o una casa donde las maltratan físicamente antes de detenerlas y deportarlas el artículo cubre las declaraciones de otras muchas víctimas Pero bueno tampoco es mi intención aquí hacer el

episodio más macabro de lo necesario ya os imagináis que las experiencias de los demás son parecidas y además Bueno pues os dejo enlazado el artículo para que podáis leerlo al completo en fin que mucho cuidado si planteáis ir a disfrutar del mundial acatar especialmente si pertenecéis a la comunidad lgtb también la lección aprender de que es que uno puede ser que puede ser quien quiera online no no hay que fiarse en absoluto de un perfil en una aplicación de este tipo porque puede estar detrás cualquiera en Qatar Puede que sea la policía pero en tu país puede que sea un mal nacido que tiene planes similares siempre conviene citarse en espacios públicos avisar amigos de dónde estás en todo momento quizá compartiendo tu localización en directo y simplemente pues tener sentido común Esto sí muy bien acabar con recomendaciones Martín porque es muy preocupante este tema y me venía la mente nuestra querida expresión no bueno que usamos a veces no siempre se tiene que usar pero tu modelo de amenazas No estás acostumbrado a que estás en tu país en tu provincia donde sea en tu estado Incluso en Estados Unidos cada uno tiene un poquito diferencias no pero bueno estás acostumbrado a que sabes cómo funciona el tema y los temas de privacidad que hay y no la libertad de expresión Y tal Pero cuando vas a otro país cuando viajas ya sea por trabajo por placer o lo que sea es está bien documentarse sobre todo últimamente que el mundo cambia tanto tan rápido y la tecnología también ayuda mucho a abusar de la privacidad y todo lo que pongas en tus redes sociales como Cuando entras en Estados Unidos no que que a veces no siempre pero la policía de la frontera Pues según dicen te requisa te mira todos tus dispositivos electrónicos no ahí pueden una de dos ver lo que llevas y saber realmente quién eres o incluso instalarte implantes para luego seguirte espiarte Pero bueno también a veces dicen que les tienes que dar tus alias de redes sociales Así que también te pueden ver así que mucho mucho cuidado también cuando se viaja por el mundo el tema es que uno está acostumbrado a la zona de Confort de los del modelo de amenazas que tenemos y me he protegido tengo configurado mi teléfono y tal o mi portátil de alguna forma que aquí me sirve pero en otro sitio no me sirve es completamente distinto escenario tienes que comprarte no sé teléfonos y portátiles de un solo uso y bueno cambiar un poquito la mentalidad sí que Qué buenos apuntes simplemente Bueno un poco eso sentido común y ser consciente que online uno puede ser quien quien quiera y disfrutemos todos pero pero con cabeza y luego el otro tema que quería comentar justo que se me iba a olvidar justo hace ayer le comentaba con unos con unos compañeros también que justo es cuando has dicho el nombre o sea no me salía la noticia no la asociaba con esta noticia que leí hace poco pero hemos dicho a Jane es que justo ayer creo que fue ayer que vi una noticia sobre esta persona que salía en los medios y que lo habían identificado como un el líder de una empresa de hackford High como tú has dicho pero es que hace dos días Eso fue hace tres días o cuatro y hace dos días bueno hace tres o cuatro días se dijo que esta persona trabajaba en una empresa Big Ford que es una empresa de esta es de consultoría y auditoría que ofrece servicios de seguridad Claro pero es que hace dos días bueno Y eso Aparentemente es verídico y tal bueno Según dice no a que creerse los medios no pero hace dos días dicen que lo han echado es que obviamente Sí sí se han enterado que una empresa está haciendo site Job es como no sé por la mañana es el típico caso este estereotipo no durante el día trabajo de 9 a 6 lo que sea haciendo mi trabajo de oficina y por la noche soy malo sí y no decía lo de consultor si sí claro porque no me creyese los medios sino un plan de que es esa pantalla No ese es como como rollo Superman por el día es periodista pero luego por la noche se pone la capa lo que pasa es que este de manera negativa justo Igual queremos hacer un breve inciso para darle las gracias a nuestro patrocinador brawler que nos apoya en el podcast y que hace unas semanas

acaba de lanzar un servicio en la nube para proteger tu infraestructura en aws hablamos de brawler pro y sus ass el servicio gratuito más completo de seguridad para aws Problem Pro está construido sobre la Popular herramienta opensores frawler y además por el mismo equipo de ingenieros si ya conoces brawler que está disponible en github seguro que vas a las bondades que ofrece prowler Pro en cuestión de minutos tendrás resultados del estado de seguridad de tu cuenta de aws podrás mejorar tu postura de seguridad a través de múltiples dashboards que te permitirán ahorrar tiempo y tener una visión completa del estado de tu infraestructura puedes empezar a usar prowler pro de forma totalmente gratuita en brawler punto Pro PR owler.pro desde ya y bueno una vez dicho esto dentro noticia esta noticia que traigo de primeras parece más enfocada a equipos de respuesta de incidentes a personas que hacen investigación de malware y temas similares aunque como Vais a ver esta noticia nos afecta a todos recientemente la empresa de ciberseguridad alemana positive Security ha publicado una investigación en la que documenta como herramientas que ayudan a investigar eventos de ciberseguridad pueden exponer de hecho información sobre los usuarios atacados o las víctimas y esta información es confidencial y sensible como Vais a ver ahora cuando lo comenté en detalle no sé si alguno de nuestros oyentes se encuentran en esos equipos de respuesta incidentes pero para los oyentes que no conozcan este tipo de equipos Bueno pues voy a explicar un poquito y se dedican a como dice el nombre responder a incidentes es decir son una función de ciberseguridad reactiva y se dedican a responder a arreglar y recuperarse de un incidente de ciberseguridad estos equipos normalmente que trabajan bajo mucha presión cuando están respondiendo a incidentes porque imaginaos en un ataque de ransomware el tiempo es esencial se requiere una respuesta inmediata por lo que en muchos de estos casos lo ideal y lo que se busca Es la rapidez y precisión de respuesta un humano puede responder a incidentes no pero todos somos humanos y cometemos errores y Comparado con procesos automáticos los humanos somos lentos casi tortugas para conseguir responder de forma rápida y precisa Entonces se diseñan procesos definidos con mucho detalle y en cada paso se especifican los comandos datos de entrada y de salida y potenciales escenarios esperados y similares los denominados playbooks de respuesta a incidentes bueno Total que todo esto al estar tan definido se puede correr en procesos automáticos que permiten que la respuesta sea veloz y exacta según nist el Instituto Nacional de estándares y tecnología de Estados Unidos un plan de cuesta incidentes tiene cuatro fases que son las siguientes la primera preparación en la que te tienes que asegurar de tener capacidades de inteligencia de amenazas y detección de que hayas definido un equipo de respuesta incidentes los roles responsabilidades que tengas la infraestructura requerida las apis de sistemas de análisis de malware en archivos urls y similares la fase 2 detección y análisis cuando recibes una alerta de una potencial detección de un incidente de seguridad tienes que determinar si ha ocurrido o está ocurriendo o va a ocurrir analizar Los indicadores de compromiso que pueden ser direcciones IP nombres de sistemas y similares empezar a documentar el incidente definir una prioridad notificar a los equipos afectados y actividades similares la fase 3 es contener eliminar y recuperarse en esta fase se intenta detener actividad maliciosa para prevenir mayor impacto y también se intenta eliminar y arreglar la causa raíz y restaurar todos los sistemas para recuperar las operaciones y el negocio en la última fase la 4 tenemos las lecciones aprendidas u oportunidades de mejora que es cuando te sientas con todo el equipo y reflexionas sobre lo que ha pasado y Qué medidas proactivas se pueden implementar para evitar incidentes similares en el futuro y también Cómo mejorar el playbook de respuesta incidentes entre otros Pues en esta noticia me voy a enfocar de hecho esta noticia va sobre la fase 2 de un plan de

respuesta incidentes en la que se realiza la detección y análisis del incidente como he dicho en esta fase se utilizan muchas herramientas para analizar Los indicadores de compromiso del incidente como pueden ser la dirección IP el nombre del sistema de dns la URL incluso binarios no el tipo de archivo que es un ejecutable o un de oficina de documentos haches ingeniería inversa y similares en concreto para las urls aunque se puede usar también para direcciones IP o nombres de sistema se pueden usar herramientas online tipo virus total URL void las propias de sistemas edr en Point detection en response o incluso URL scan.io y es esta última urlscan.io sobre la que los investigadores han identificado un fallo de exposición de datos confidenciales Bueno tanto rollo pero qué es urlscam.io pues es una sandbox para la web es decir analiza y escanea urls de varias maneras principalmente para detectar sitios web maliciosos como sitios de phishing ransomware y similares esto el análisis lo puede hacer de Tres formas distintas o puede ser iniciado digámoslo así de Tres formas distintas la primera es los servidores de urlscam.io tienen procesos que automáticamente van escaneando todas las urls que encuentran por internet no el segundo la segunda vía sería que un usuario manualmente va a urlscam.io lo ponen en el navegador y en el campo de texto introduce la URL que quiere analizar y la envía y la tercera forma en la que se inician los análisis de urls es a través de apis que permiten la integración con productos de ciberseguridad esta última opción es la que principalmente conduce a la fuga de datos confidenciales aunque también podrían darse fugas de las otras dos formas no que un usuario suba la URL con datos confidenciales sin darse cuenta o que en internet hay alguna URL con datos confidenciales que también se puede dar el caso cuando buscas en Google también te puedes encontrar de vez en cuando con urls que sean cacheados se han guardado en el servidor de Google y devuelve resultados con esa darle con datos confidenciales para cada análisis de URL el servicio urlscam.io proporciona la siguiente información primero la URL enviada con todos los parámetros get y lo que esto significa ya lo podéis pensar lo segundo es la url efectiva en caso de una redirección no sé si os habéis dado cuenta que a veces cuando ponéis el nombre de una URL por ejemplo google.com pues te puede redireccionar a www.google.com Este es un caso sencillo pero se puede dar el caso de que haya más redirecciones no sé se pueden haber no es que hayan dos redirecciones puedan en 3 4 las que el sitio web considere necesario también el análisis proporciona cualquier solicitud http que se haya realizado mientras se escaneaba la URL esto significa que todos los documentos los objetos de la página web también sean capturado y también se ofrece información sobre las ips y dominios relacionados con la URL y todas las urls dentro de esta página web que se descarga vía http también se proporciona una captura de pantalla de la página tomada en el momento del escaneo y finalmente se proporciona la respuesta html completa del sitio web visitado de la URL URL scan junto con otras herramientas de análisis de indicadores de compromiso se pueden utilizar de forma manual Aunque para conseguir la respuesta rápida y precisa su uso se ha extendido a productos que automatizan el análisis y ahora se incluyen en sistemas de respuesta automatización y orquestración de seguridad los sistemas que se conocen como soar por sus siglas en inglés de Security yorkstation automation en response la página de documentación de urlscam.io enumera integraciones de su Api con 26 soluciones Shore comerciales como Palo Alto s planck rapid Seven fire eye y ark Side y también con 22 proyectos Open source utilizados para temas de osint y librerías para conectarse a la Api de borrar scan.o en concreto lo que significa que hay otras muchas aplicaciones no identificadas que pudieran estar utilizando el servicio de urlscam.io Pues cuál es el problema Pues en este caso los sistemas short sistemas de análisis de emails o incluso alertas automáticas de cualquier tipo no

van a saber si en una URL hay información confidencial y van a iniciar un análisis en urlscam.io enviando la URL con esta información que contiene Porque estos procesos automáticos hoy en día no tienen ninguna regla configurada para que no se envíe una URL que contenga un parámetro get que se llame password Así que o similares No ya os hacéis la idea seguro que después de esta noticia o este caso igual van a implementar estas medidas para evitar enviar urls con datos confidenciales Pero bueno echa la ley echa la trampa no un atacante podría también en su link en su URL de fishing incluir un parámetro que se llama password para intentar saltarse que un sistema sou hmn envíe la URL a estos sistemas de análisis como wordlesscam.io sí estos sistemas son implementan esta medida que todavía no está implementada pero es un caso hipotético que comento bueno como digo en los sistemas shorts sistemas automáticos de análisis de emails o incluso alertas automáticas lo que hacen es enviar la URL a urlscam.io no esto lo que va a causar es que por ejemplo por cada email que un usuario reciba los sistemas de seguridad automáticos van a buscar urls en el cuerpo del email e incluso en los archivos adjuntos y realizar un análisis de forma automática en urlscam.o en base a estas urls identificadas y justo Los investigadores se pusieron a investigar se pusieron a buscar en urscam.io y encontraron urls confidenciales de diversos tipos que me dejaron de nuevo no estamos en Halloween pero me dejaron con muchos escalofríos porque habían urls por por ejemplo para reseteo de contraseñas urls para creación y confirmación de cuentas urls con claves de apis de servicios Online urls para invocar funciones de robots de Bots en sistemas de mensajería como Telegram urls para acceder a documentos confidenciales como peticiones de firma de Doki usain urls para acceder a documentos compartidos en sistemas en la nube como Google Drive o iCloud a los que cualquiera puede acceder solo con tener dicha URL otras con enlaces para archivos enviados vía dropbox algunas que incluían invitaciones a sharepoint otras con invitaciones a unirse a suscripciones de pago como los servicios de Apple invitaciones a eventos corporativos de Apple por ejemplo urls con enlaces a vídeos no listados de plataformas online estilo YouTube y bueno una lista para no parar pero lo dejo ahí porque si no no acabo el episodio muchos de los análisis que contienen este tipo de urls confidenciales desaparecen de los resultados después de 10 minutos Pero uno puede poner puede realizar búsquedas de forma continua con filtros específicos no como los que se conoce como Google doc no como site dos puntos in URL dos puntos No pues en urlscam.io También tienen otras palabras otras keywords otras sintaxis para buscar y por ejemplo si pones page punto domain dos puntos y pones lo que es El dominio que quieras por ejemplo apple.com pues eso lo que te hace es que te sale te busca te da los resultados de todos los análisis de urls que contengan El dominio apple.com bueno el tema es que aunque desaparezcan los resultados después de 10 minutos uno puede crearse su automatización y visitar la página web donde están el con una búsqueda específica Y todavía encontrar resultados de este tipo del dominio apple.com por ejemplo Durante los primeros 10 minutos después de que se haya realizado y publicado en el análisis y antes de que se borre este tiempo de borrado de 10 minutos De hecho estaba relacionado con urls de Apple específicamente y los investigadores se enteraron después de que Apple requiere que sus dominios se excluyan de los resultados de análisis aunque esto URL scan punto a ello lo ha implementado mediante el borrado periódico cada 10 minutos de todos los análisis que tengan sus dominios la forma más efectiva hubiera sido hacer todos los escaneos de urls de Apple privados Aunque igual esto requeriría una cuenta de pago y obviamente si eres un usuario normal y no quieres pagar por este servicio y envías una URL que tenga apple.com Pues claro no podrías disfrutar de este servicio impacto pues una de las muchas partes críticas en los

resultados publicados de los análisis de las urls en urlscan.io son bueno la URL en concreto pero más en concreto son los parámetros get de esta URL que pueden contener nombre de usuarios contraseñas Bueno aunque en El Siglo 21 esperamos que esto ya no pase que no se envíen contraseñas como parámetro get en una URL verdad también se pueden encontrar tokens de autenticación que pueden tener una larga duración o no y otros temas similares Las capturas de pantalla también son muy preocupantes obviamente y Bueno ahí lo dejo no para que tengáis una idea ya veis que hay bastante riesgo si estas herramientas automáticas tipo short o usuarios de la Api están realizando análisis de urles y los resultados se muestran de forma pública esto puede causar una fuga de datos confidenciales muy grave y como estas herramientas de seguridad avanzadas se instalan principalmente en grandes corporaciones y organizaciones gubernamentales la información filtrada podría ser muy delicada a raíz de esto Los investigadores se quedaron pensando si podrían encontrar algo más si podrían rascar un poquito la superficie de esta este incidente no que descubrieron y lo que hicieron fue lo siguiente primero recolectaron algunas de las urls de los análisis y contactaron a los usuarios afectados vía email notificándoles de que esta URL se encontró en urlscam.io o sea haciendo una acción noble verdad Pero también añadieron una URL de seguimiento en el email con buenas intenciones Obviamente con esto lo que querían saber era si realmente los usuarios eran los que enviaban las urls a urlscan.io o si por el contrario en las herramientas automáticas de tipo sol y después de su análisis validaron su sospecha de que en el 50% de los casos son las automáticas las que envían la URL a urlscam.o inmediatamente después de recibir el email de todas formas solo enviaron hicieron una muestra una prueba a unos Entre 10 y 20 usuarios si no recuerdo mal Así que no igual No es una muestra significativa para concluir que el 50% de los casos vas a tener éxito digamos en en encontrar que un una herramienta tipo short envía de forma automática la URL a urls.ao pero hay que dar el dato no los investigadores querían seguir un poquito encontrando más indagar y buscar más y de hecho querían saber qué tipo y fabricante de short se encontraba detrás de estas peticiones auerdescant.io para analizar las urls y con esta duda Los investigadores pidieron a urlscan junto a ellos si podían compartir con ellos los user agents esta cabecera http que envía en todas las peticiones http de los usuarios a los que los investigadores les estaban haciendo el seguimiento con esta información Los investigadores descubrieron los shorts que filtran las urls confidenciales que son los siguientes Palo Alto xor swim Lane IBM Security cureyder sour antes conocido como IBM resilient s planksore antes conocido como s planck Phantom y dimension así que queridos oyentes si usáis alguno de estos o sabéis si vuestra empresa los usa y da mirar la configuración ahora mismo para no liquear detalles importantes al mundo en general Y qué podría hacer un cibercriminal un atacante si consiguiera apoderarse de estas urls confidenciales que se envían a urlscam.io No pues hay diferentes casos de abuso desde el típico spam no multi criminal podría recopilar direcciones de correo electrónico y otra información personal para utilizarla en ataques de spam también podrían recabar información de email y similares para realizar campañas de fishing increíbles y bueno en temas también de red timing como Martín y yo hacemos y similares pues se puede utilizar esa información para encontrar portales de administración ocultos igual obtener un primer punto de apoyo o pivote hacia la red interna o hacia la aplicación que quieras un poquito testear o enfocarse en objetivos potenciales pero en caso de abuso interesante es el robo de cuentas y recapitulo para el 50% de los usuarios que reciben correos electrónicos los las herramientas soar lo que van a hacer es inspeccionar el email y coger todas esas urls que contienen los emails y enviarlas a urlscam.io para su análisis inmediatamente después de recibir

el email y debido a que todo esto se hace de forma automática a través de estas herramientas short que tienen configurado la petición el envío de la del análisis de la URL vía la Api de burlescan.io con un análisis público pues van a exponer directamente esta URL como pública en el servicio urlscant.io de esta forma cómo puede un atacante sacar provecho de este escenario de esta de este fallo pues lo primero es sería identificar el email del objetivo que esto se puede sacar mediante osint bases de datos de fugas de información online ingeniería social El segundo paso sería determinar En qué servicios tiene cuenta con ese email y bueno y centrarte en las que en las que quieras robarle su cuenta por ejemplo Gmail o lo que sea el tercer paso sería resetear la cuenta en servicios Online para que la víctima reciba el email de reseteo de cuenta reseteo de contraseña y su short envía la URL de reseteo de cuenta o contraseña inmediatamente a urlscam.io el siguiente paso es Buscar las urls de reseteo de cuentas en urlscam.io como he dicho se puede poner se puede utilizar este keyword page punto domain dos puntos y El dominio que quieras un poco atacar si es google.com Pues ahí está o apple.com o el que sea y bueno la encuentra el cibercriminal ya es suya y ahora pues lo que puede hacer es resetear la cuenta y a poder esa de ella así que ese sería un escenario de ataque bastante eficiente bastante eficaz de llevar a cabo quiero comentar un poquito no todo el pánico sino también lo bueno que mitigaciones por una parte urlscam.o.io hizo lo siguiente contacto a muchas de las entidades afectadas que los investigadores identificaron para comentarles suceso y que arreglarán este este problema de visibilidad el segundo acto que hicieron fue Añadir más reglas de borrado de análisis públicos en función de urls confidenciales es decir como el tema de Apple que pidió aurles camp.io que borrara todas sus urls públicas después de 10 minutos de haberlas publicado Pues lo mismo para otras que words punto ha visto que pueden contener también datos confidenciales no como reseteo de contraseñas y todo toda la lista que he mencionado anteriormente queda escalofríos lo Okay workscan hizo fue Resaltar el tema de visibilidad de la visibilidad de los resultados de los informes de los análisis de urls en la web en su web y en la documentación de la Api en plan en mayúsculas Cuidado con la visibilidad del Análisis ponlo en privado o si no atente a las consecuencias y lo último también que hizo fue publicar un blog llamado mejores prácticas para la visibilidad de análisis de urls de la parte de usuarios qué podemos hacer como usuarios pues definir asegurarse de que la visibilidad de los análisis que enviamos a words.ayo son privados y esto se puede especificar en cada petición http vía parámetros de Lápiz o cuando vas a la web también de forma manual lo segundo que se puede hacer es informar a urlscam.io de análisis que no deberían ser públicos mediante el botón de report que está en cada análisis en cada página de análisis y lo tercero que podemos hacer es contactar a urlscam.io para que elimine resultados que no queréis como lo haríais con Google cuando sale algún tipo de información personal en Google se le puede enviar una petición para que lo elimine de su servidor Pues en urls.io si se encuentra algo por ejemplo que no tenga el botón este de Ripoll Pues también contactarles y esto no es la primera vez que pasa por ejemplo a principios de este año un incidente similar expuso datos de repositorios privados de github para los que no conozcáis git up es este repositorio de código principalmente Aunque hay gente que lo utiliza para bueno alojar texto datos no hace falta que sea código no pero principal es código porque tiene tema de control de versiones cuando creas un documento pues y creas otro nuevo te guarda el histórico de todos los cambios de estos documentos en cualquier caso una un servicio online muy usado a nivel mundial por millones y millones de usuarios y a principios de año lo que pasó es que un fallo similar lo que hizo fue exponer la URL del repositorio de repositorios privados de github y también el nombre de usuario

del dueño del repositorio github se enteró de un incidente de este incidente interno por parte de un empleado de github en que los sitios web de github pages en concreto páginas de github publicados desde repositorios privados en github se enviaban a urscam.io para analizar los metadatos como parte de un proceso automatizado git have lo que hizo al respecto fue arreglar este proceso automático que enviaba los sitios de Quizá pages para análisis de metadatos de tal forma que solo se envíen para el análisis los sitios públicos de quizás pages y no los privados además de pedirle ahorrescan.io que elimine todas los análisis anteriores de repositorios de quizás privados que se habían expuesto y de hecho esto fue la motivación de los investigadores que les llevó principalmente a realizar su análisis su informe su investigación Aunque en este caso el tema de github un poco también como en el caso actual había que tener un poco automatización al respecto porque las urls también desaparecían de borrescard.io después de 30 segundos de haberse publicado en el análisis en el caso de este este incidente más reciente en el caso de Apple la urls los informes desaparecían después de 10 minutos y porque la había pedido Apple Pero bueno todas las otras los otros dominios no se hacía nada al respecto O al menos no consta como tal por parte de los investigadores Aunque bueno había que habría que preguntarle un poquito más a urlscan.io si tiene tenía más reglas de este tipo de borrado aunque como he dicho vr scan.io ha mejorado el tema y ha añadido muchas más de Esas reglas de borrado de análisis de urls que son públicas y con esto queridos oyentes llegamos a la pregunta del episodio crees que estas herramientas como urlscam.io de análisis de indicadores de compromiso de gestión de incidentes deberían estar disponibles para todo el mundo tenemos cuatro respuestas la primera es sí Y además gratis La segunda es no solo para empresas o gobiernos es decir solo para entidades autorizadas la tercera es no solo de pago y la última es no nunca así que ya sabéis ir a Twitter y os invitamos a votar me ha encantado la noticia de hecho Alexis me ha recordado a un reporte de background y que envié yo yo creo que lo había mencionado ya alguna vez en el episodio pero fue como dinero no fue mucho creo que me dieron no sé mil dólares o algo así pero era en torno a esto a secretos almacenados en las urls que no solo liquean en el historial del navegador no solo pueden ser indexadas sino en este caso lo que pasaba era es que era a través de la cabecera de reference del protocolo http que bueno es una cabecera que se suele utilizar para temas de marketing Y tal Pero cuando tú en un dominio por ejemplo estás en por decir algo en google.com tú le das a un enlace que va a Martín vigo.com yo cuando llega a San Martín vigo.com puede ver puedo ver que vienes desde google.com de hecho en concreto la la URL exacta desde dónde vienes en google.com Entonces yo Esto se lo reporté a una aerolínea que cuando tú vas a hacer el check-in en una aerolínea no normalmente la URL contiene tu apellido y el localizador del billete que realmente es la manera de autenticarte para poder cambiar las reservas poner el pasaporte lo que tú quieras pues me di cuenta que había lo típico del sistema de cuando necesitas ayuda no el botoncito quieres ayuda o soporte y le di y esta aerolínea en concreto era United Airlines había contratado un servicio de terceros para que pues gestionar todo el tema de cuando la gente está haciendo check in y algo no funciona Entonces al darle a Ese botón eso cargaba pues no me acuerdo que dominio era pero uno tercero pero vi que se estaba enviando la URL de la aerolínea que contenía el secreto para poder cancelar mi vuelo y todo o sea esa empresa de terceros que habían contratado sus servidores estaba recibiendo miles y miles de urls de United Airlines que contenía el apellido y el localizador del billete que eso permita cualquiera acceder a la información de tu pasaporte tus datos personales y todo esto y es que fue súper fácil de de encontrar porque no tiene mucho técnico tenía ahí el burp corriendo y ya está y me dieron que sí

creo que como mil dólares o algo así muy interesante para para usarlo en un viaje a una conferencia Sí aquí para venir hasta albacete que esto está lejos tío pero pero sí muy interesante tu noticia eres si la verdad que alguna vez lo he visto también y me pregunto realmente el siglo XXI ya se usa no te puedes fiar porque el rifer lo puede modificar cualquiera deberían fiarse de la Cookie de sesión que debería estar descifrada o con integridad de para prevenir modificación pero ese campo No sé todavía quién lo usa para que el tema de analíticas como he dicho tú claro justo justo De hecho si para saber desde dónde te linca la gente y todo esto pero claro hoy en día la mayoría de navegadores es una de las cosas que te quitan ya automáticamente navegadores como firefox Y esto es que digamos que están orientados a la privacidad Pues eso lo quitan y ya está directamente y luego el otro comentario es creo el comentario el caso de abuso este que he comentado de robo de cuentas también es un poquito parecido a tu herramienta verdad la de funerator era que también hacía algo similar con lo de Siri y tal Ah hablas de la de la de ranson Ball Sí claro bueno perdón no es que son muy malos eligiendo nombres Ya lo sé Alexis ya lo sé pero sí Bueno esta era Era no tiraba tanto de urls para sacar los secretos Claro pero pero lo que dices tú es como maneras inseguras de enviar material de bueno credencial materia al me sale digamos bueno información sensible no respecto a tu autenticación como el nombre de usuario y contraseña entonces a veces Pues claro no no pensamos que ponerlo en una URL pues eso es que puede acabar en sistemas de casing en el historial de tu navegador en la cabecera del referer y en otros tantos casos hay sitios Sí pues pues lo dicho para los que estéis en grandes empresas Y uséis estos sistemas soar que tiran de urls.io ir a mirarlo ya para evitar mayores madera esto es una de estas noticias que has dado que porque muchas veces buscamos noticias que no afecta a la gente por ejemplo la que digo antes que pues la mayoría no van a ir a catar o cuando hablamos de vulnerabilidades más de por parte de gobiernos contra Vips Pero esto seguro que hay mucha gente en departamentos de it y tal responsables que a lo mejor esto le ayuda van y dice Mostrar por lo tenía público O sea que si alguno por favor hacérnoslo saber no nos tenéis que decir la empresa ni mucho menos pero un poco por tener esa satisfacción de que la noticia de Alexis pues ha servido en caso Real de ostras lo he escuchado en el podcast he ido a mirar y mira Pues nosotros nos estaba afectando Sí sí nos encantaría que se os haya servido esto para mejorar vuestra seguridad así que de hecho worlscan ha contactado como he dicho algunas empresas afectadas pero no sé si han llegado a países no anglosajones no no no de habla inglesa Así que desde aquí pues hacemos un poco la labor ahí está la protección los hispanohablantes están pocos seguros pues hasta aquí ha llegado el episodio yo me despido desde albacete como siempre agradeciéndoos que estéis ahí hasta el final de verdad es un auténtico placer ir conociendo en persona a los oyentes mañana iré con más pegatinas pero muchísimas gracias como siempre por quedaros hasta el final apoyarnos seguirnos en redes sociales como siempre recuerda Alexis y nada nos vemos y nos escuchamos en el próximo episodio Muchas gracias a todos que lo paséis bien y que los que veáis a Martín que disfrutéis con él y nos vemos en la próxima para la siguiente te vienes Alexis Adiós adiós chao chao si te ha gustado este episodio y quieres ayudarnos a seguir con el podcast compártelo con tus amigos y compañeros con tu apoyo podremos atraer y despertar el interés por la ciberseguridad de mucha más gente Acuérdate de dejarnos un comentario y una valoración donde nos estés escuchando también puedes seguirnos en Twitter Instagram y Facebook te esperamos en el próximo episodio de tierra de hackers