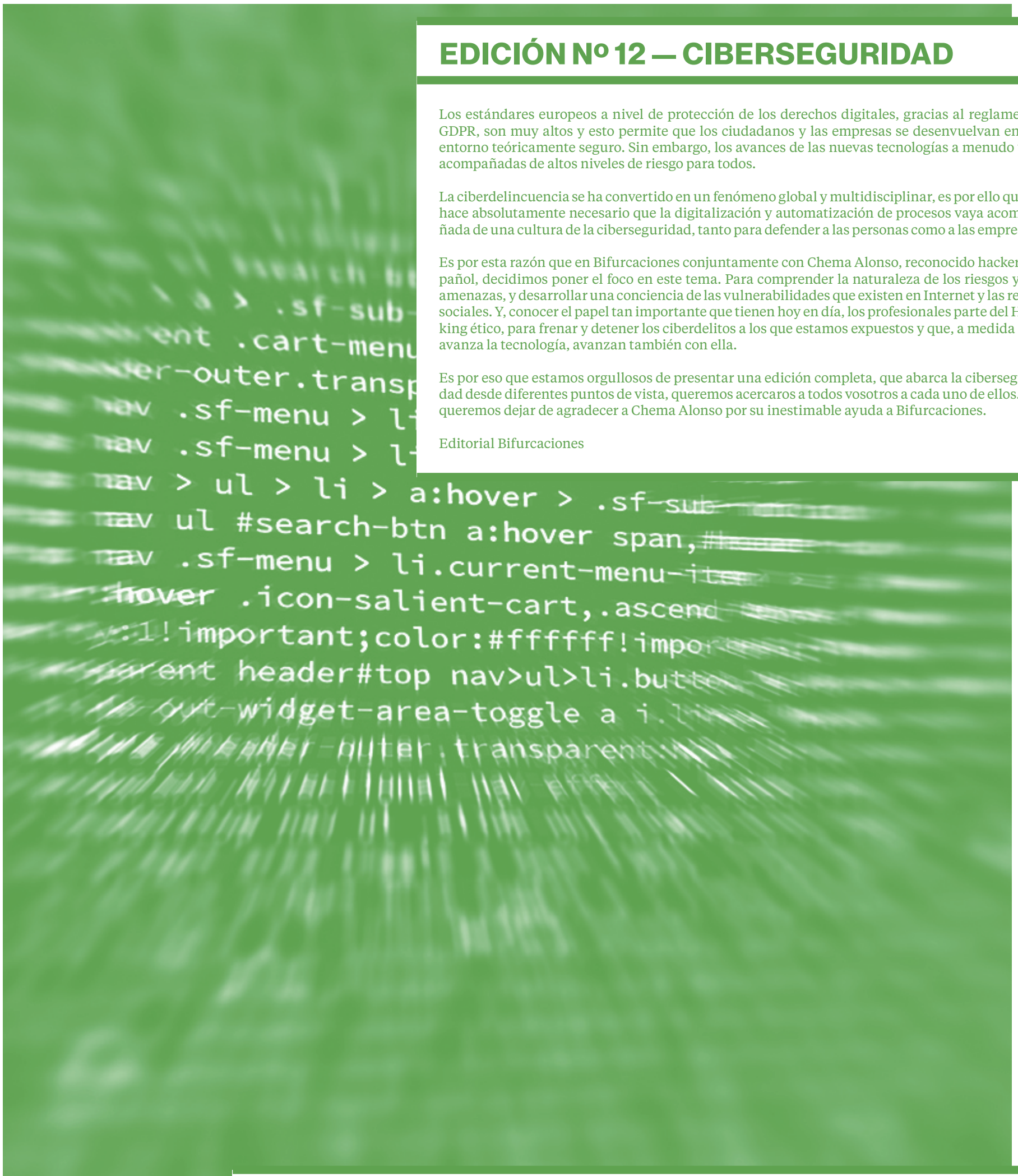
EDICIÓN Nº 12 - ENERO/FEBRERO 2022

BIFURCACIONES

1hv.co

by 1hv

BIFURCACIONES.COM



EDICIÓN Nº 12 — CIBERSEGURIDAD

Los estándares europeos a nivel de protección de los derechos digitales, gracias al reglamento GDPR, son muy altos y esto permite que los ciudadanos y las empresas se desenvuelvan en un entorno teóricamente seguro. Sin embargo, los avances de las nuevas tecnologías a menudo van acompañadas de altos niveles de riesgo para todos.

La ciberdelincuencia se ha convertido en un fenómeno global y multidisciplinar, es por ello que se hace absolutamente necesario que la digitalización y automatización de procesos vaya acompañada de una cultura de la ciberseguridad, tanto para defender a las personas como a las empresas.

Es por esta razón que en Bifurcaciones conjuntamente con Chema Alonso, reconocido hacker español, decidimos poner el foco en este tema. Para comprender la naturaleza de los riesgos y las amenazas, y desarrollar una conciencia de las vulnerabilidades que existen en Internet y las redes sociales. Y, conocer el papel tan importante que tienen hoy en día, los profesionales parte del Hacking ético, para frenar y detener los ciberdelitos a los que estamos expuestos y que, a medida que avanza la tecnología, avanzan también con ella.

Es por eso que estamos orgullosos de presentar una edición completa, que abarca la ciberseguridad desde diferentes puntos de vista, queremos acercaros a todos vosotros a cada uno de ellos. No queremos dejar de agradecer a Chema Alonso por su inestimable ayuda a Bifurcaciones.

Editorial Bifurcaciones

Protección de datos | Derechos digitales

CIUDADANOS DIGITALES Y ATERRORIZADOS: HABLEN CON SU TATARABUELO

Martín Sacristán

Escanea este QR

Periodista y escritor.

Miembro del consejo editorial de Bifurcaciones. Narra la actualidad contemporánea cada semana en JotDown. Escribe sobre ciencia y tecnología del deporte para el Barça Innovation Hub del F.C. Barcelona. Colabora en la revista El Ciervo. Es autor de libros de ensayo y ficción.

Las corrientes de opinión sobre la tecnología se han alternado en nuestra sociedad, oscilando entre la esperanza y el pesimismo, desde que empezamos a trabajar con máquinas. Ahora, convertidos en ciudadanos digitales por esas nuevas formas de relacionarnos con las empresas, la administración, y el ocio, vuelve a predominar el miedo.

Los periodistas culturales de nuestro país son una de sus más claras manifestaciones. El 70% son tecnopesimistas. Y porqué debería importarnos la sección cultura. Porque crea y exacerba una corriente de opinión que es, además, tendencia mayoritaria en la ficción. Con tres ejemplos muy recientes, Upload (serie de Amazon), No mires arriba (película en Netflix) y El sueño chino, de **Ma Jian**, Random House.

Dos preocupaciones dominan, la distante, creer que robots e inteligencias artificiales nos dejarán sin trabajo; y la inmediata, que la cesión de nuestros datos personales nos convierta en rehenes de las tecnológicas, o en elementos de un estado que vigile hasta nuestras actividades más íntimas. Y al menos en Europa, esta preocupación no está justificada.

La UE es la mayor protectora de los derechos digitales gracias al Reglamento de Protección de Datos Europeo, el GPDR. Todas las apps y desarrollos tecnológicos se han adaptado a esa regulación. Somos un referente en ciberseguridad, entendida en su sentido más amplio, como protección de la actividad digital en todas sus facetas.

Lo acabamos de ver con el órdago de **Zuckerberg**, avisando que apagaría Facebook e Instagram en Europa si no le permitían llevarse a EE.UU. los datos de sus clientes. Cuando el primer ministro francés **Bruno Le Maire** y el de economía alemán **Robert Habeck** le respondieran que podríamos vivir muy bien sin Facebook, la compañía desmintió haber dicho tal cosa. Lo relevante, aquí, no es la enésima anécdota de Meta, sino que estos dos mandatarios hayan expresado esa opinión generalizada, ligada al temor, de que los productos de las tecnológicas nos perjudican.

Un temor irracional, porque la seguridad existe, y los datos están controlados en cualquiera de los tres modelos de ciudadanía digital. En el chino autoritario, donde los datos del ciudadano digital pertenecen al estado. En el estadounidense, que los ha dejado en manos de las empresas privadas, aunque ahora muchos estados tradicionalmente demócratas, como California, hayan empezado a introducir regulaciones semejantes al GPDR. Y finalmente, en el europeo, donde los datos son privativos del ciudadano. Regulaciones distintas, medidas efectivas, y un mismo miedo compartido por los ciudadanos de estas tres ciudadanías digitales tan distintas entre sí.

Entenderemos mejor porqué si hablamos de **Lord Byron**. El poeta inglés, sí. Excesivo como era, y arrasado por los escándalos en la puritana sociedad británica, decidió largarse de allí en la primera autocaravana de la historia. Recorrió Europa, se asentó en Italia primero y luego en Grecia. ¿Saben lo único que no llevaba consigo? Un pasaporte.

Tan solo hace cien años que estructuramos los estados con documentos que nos convirtieron en ciudadanos exclusivos de países. Pasaportes ligados al lugar de nacimiento, DNIs identificativos, números de la seguridad social. Byron diría que nos han tiranizado. Ahora la tecnología nos hace dar un paso más, y los estados nos convierten en ciudadanos digitales. Y no podemos ser ingenuos. El margen de libertad absoluta que restringieron aquellos documentos «tiránicos» se reducirá aún más ahora. Cosas como mantener el anonimato en un espacio público o pagar en B serán casi imposibles. Otra cosa es que eso vaya a conducirnos a una distopía.

Nuestros estados estructurados con ciudadanías legales han facilitado el bienestar, y la evolución tecnológica puede traernos un bienestar aún mayor. En cuanto a los datos, a menudo olvidamos los que debemos entregar para adquirir la condición de ciudadanos adultos. Si pudiéramos explicar a nuestro tatarabuelo que al emitir el DNI la policía registra nuestras huellas digitales, nos preguntaría bajo qué clase de tiranía opresora estamos viviendo.

Pero el tatarabuelo empezaría a dudar cuando le explicáramos que también entregamos nuestros datos a empresas a cambio de suscripciones gratuitas a información o aplicaciones. Gratis no, matizaría, por un intercambio, admisible si es justo. El tatarabuelo no necesitaría explicaciones para entender por qué nuestra imagen en internet, todo lo que hemos subido como comentarios, fotos, etc. constituye un perfil que puede condicionar nuestra contratación, participación política, etc. Él también se preocupaba de tener una imagen de buen ciudadano, yendo a los servicios religiosos y cuidando dónde hablaba mal contra el rey.

Vivimos un proceso histórico tan decisivo como el de nuestros tatarabuelos, porque vamos a convertirnos masivamente en ciudadanos digitales. Para hacer esa transición adecuadamente necesitamos ciberseguridad, entendida en un sentido mucho más amplio que el actual. Nuestro bienestar inmediato va a depender de que esté regulada y bien diseñada, y que participe de las demandas sociales. Como europeos tendremos que defender además que eso debe hacerse desde el respeto a los derechos y las libertades ciudadanas de nuestras constituciones. Que llegaron, por cierto, después de Lord Byron. El poeta de nuestros tatarabuelos, y el primero en escribir una distopía cuando llegó aquel año sin verano de 1816. Un episodio tan impactante como nuestra pandemia, y desde el que hemos llegado a un futuro mejor.

Delicuencia informatica | Crimen organizado

ENTENDIENDO EL CIBERCRIMEN

Jorge Bermúdez González

Fiscal de la Unidad de Apoyo de la Fiscalía General del Estado.

Escanea este QR

Fiscal de la 46ª Promoción (2006), licenciado en Derecho por la Universidad de Deusto. Delegado de Criminalidad Informática en la Fiscalía Provincial de Guipúzcoa desde octubre de 2007, destinado en el gabinete de la Fiscal General del Estado desde marzo de 2020, preside el subcomité de ciberseguridad para la Administración de Justicia. Profesor del Master en Ciberdelincuencia de la Universidad de Nebrija, del curso de Experto en Derecho Digital de la Universidad de Deusto y el Cybersecurity Summer BootCamp de INCIBE.

mypublicinbox.com/Ender

Efectivamente, ya hace décadas que los estados modernos destinan esfuerzos policiales y judiciales a combatir la criminalidad que campa en dispositivos informáticos y a través de la Red. En un momento primigenio, lo máximo que el investigador podía mostrarle al juez era una caja gris, la que contiene la CPU, el disco rígido, la placa base y demás componentes de un PC. Luego llegaron los dispositivos portátiles, las tabletas y smartphones, y por último, todos esos dispositivos convergieron en la nube.

Imaginemos esa escena que el cine estadounidense nos ha presentado, de forma recurrente, en films noir de todo pelaje: ese detective de la policía que llega al lugar de un crimen, y se encuentra con un cadáver.

-Johnson, homicidios, ¿qué tenemos?

-Varón caucásico, veinticinco años, múltiples puñaladas.

Ya de vuelta a la realidad, y más concretamente a la española, la escena probablemente se produciría ante el juez de guardia, figura encargada de dirigir el llamado “levantamiento del cadáver”.

Lo que nunca veríamos, ni en la ficción cinematográfica, ni en nuestra prosaica cotidianeidad, será que alguien le tenga que explicar al protagonista de nuestra historia que allí hay, efectivamente, un muerto. Ni siquiera cuando todo lo que reste sea la arquetípica silueta marcada con tiza en el suelo, reproduciendo la posición en la que se halló el cuerpo.

¿Por qué? Pues, obviamente, porque nadie le tiene que explicar, a un policía o a un juez, en qué consiste una persona que

ya no está viva. Es una realidad dolorosamente física, concreta y palpable. Por utilizar terminología jurídica, es "perceptible por los sentidos". Sin embargo, a la hora de determinar la causa de la muerte, natural o violenta, y su etiología, accidental, homicida o suicida, sí que habrá un experto que tenga que aclarar, conforme a la lex artis de la criminalística y la patología forense, estos extremos.

Esta diferencia entre lo que el juez puede apreciar por sí mismo, y aquello que necesitará de una explicación técnica para su debida comprensión y, por ende, la aplicación de la ley, salta por los aires cuando pasamos al terreno tecnológico.

Efectivamente, ya hace décadas que los estados modernos destinan esfuerzos policiales y judiciales a combatir la criminalidad que campa en dispositivos informáticos y a través de la Red. En un momento primigenio, lo máximo que el investigador podía mostrarle al juez era una caja gris, la que contiene la CPU, el disco rígido, la placa base y demás componentes de un PC. Luego llegaron los dispositivos portátiles, las tabletas y smartphones, y por último, todos esos dispositivos convergieron en la nube.

En esos primeros tiempos, los que el investigador **Simson L. Garfinkel** llamaba "the golden age of the computer forensics"[1], solían plantearse dos tipos de problema. El primero, de tipo sustantivo, del tipo de delito. Por remitirnos a las estadísticas de evolución de la criminalidad, que publica anualmente la Memoria anual de la Fiscalía General del Estado, entre la 2ª mitad de la década 2000-2010 y la 1ª mitad de la siguiente, el segundo delito con cifras más altas en delincuencia informática era el relacionado con la pornografía infantil.

Ahora bien, a la vista de las frías evidencias físicas incautadas, el juez no iba a tener una idea clara de qué tendría delante. Insisto, sólo tendría una torre de ordenador, o incluso un disco duro aislado. Incluso si le presentara el dispositivo conectado, con la pantalla del monitor encendida, y viera las crudas imágenes, estáticas o en movimiento, tampoco podría emitir un juicio inicial.

Sí, es cierto que la pornografía infantil, ese concepto que los anglosajones rechazan, prefiriendo el más descriptivo de "child abuse material", puede llegar a ser brutalmente explícita. Pero el problema sería determinar si estamos ante un supuesto de mera posesión para uso propio o uno de difusión, incluso de producción. ¿La diferencia? En caso de tratarse de material realizado con menores de trece años, pasar de una multa económica en el primer caso, a penas de uno a cinco años de prisión en el segundo, y de cinco a nueve años en el segundo.

Para discernir entre los tres tipos, habría que comprender la tecnología que subyace a las fotografías y vídeos. Si los expertos en digital forensics sólo encuentran rastros de búsqueda y descarga en el navegador web, incluso la prueba de que ha existido visualización en la caché del reproductor de vídeo, estaríamos ante un supuesto de mera tenencia. Pero si lo que se halla es un programa cliente de una red de intercambio P2P como eMule, y los archivos de registro, como known.met o ShareDir.dat, desvelan que el sujeto creó carpetas específicamente compartidas, donde guardaba esos archivos a disposición del resto de usuarios durante semanas o meses, podríamos hablar claramente de un supuesto de difusión. Y aún más grave, si lo que encontramos en los archivos son metadatos de creación con un modelo específico de cámara, y una cámara de esas características aparece en la entrada y registro, podemos llegar a colegir que el sospechoso es culpable de un delito de producción de material pedófilo. Pero esto no se lo puede decir el perito al juez, porque existe una norma inquebrantable en Derecho: Iura novit curia, el juez conoce la ley. Los expertos pueden asesorarle sobre materias extrajurídicas, pero tendrá que ser el conocimiento tecnológico del operador jurídico el que le permita interpretar esa realidad.

El segundo problema será de índole procesal, el cómo se introduce la prueba en el proceso. Porque para llevar un disco duro ante un juez, no se puede partir del original. Toda actuación sobre ese hardware llevaría a una alteración de los datos MAC (modificación, acceso y creación). Por ello, habrá que empezar con una copia bit a bit, mediante una clonadora forense. Dicho aparato, tras un análisis inicial, escupirá una ristra de números y letras, el sumatorio hash, que permitirá compararlo con la copia y garantizar que, en el momento de empezar los análisis técnicos, ambos ejemplares eran idénticos y que, por lo tanto, una nueva copia obtenida por la defensa para una contrapericia tendrá todas las garantías.

Y esto, sólo hablando de delitos relativamente antiguos. En la actualidad, un supuesto de cryptojacking, el secuestro de la capacidad de proceso de un dispositivo, como un smartphone, para el minado de criptoactivos, eleva la complejidad en ambos ejes a un nuevo orden de magnitud.

[1]"Digital forensics research: The next 10 year", https://www.sciencedirect.com/science/article/pii/S1742287610000368

Defensa Colectiva

Estafas en Internet

EL CIBER FRAUDE HOY EN DÍA

Escanea este QR

Juan Carlos Galindo

Investigador y Perito Judicial en Delitos Económicos y Societarios

Experto en Prevención de Blanqueo de Capitales y Financiación del Terrorismo (Inscrito en SEPBLAC). Director en GALINDO LEGAL, agencia de inteligencia y prevención del delito. Presidente de honor de ASEBLAC, Asociación española de sujetos obligados en prevención del blanqueo de capitales y Coordinador del comité internacional de blanqueo de capitales de la World Compliance Association.

mypublicinbox.com/GalindoLegal

Hay miles de personas en España que diariamente son atacadas en la red y millones en el mundo. Los ciberdelitos se han convertido en una lucha sin cuartel a nivel mundial y en una de las materias prioritarias de seguridad nacional y mundial. Pero hasta la fecha, vamos perdiendo.

No hay día que no encontremos una noticia al respecto de una estafa, un robo, una usurpación de identidad o una falsificación en el ciberespacio, en algún medio de comunicación, o tengamos conocimiento de esta, en nuestro entorno más cercano. Y esto tiene un riesgo, y es que lo consideremos como algo normal, algo natural, como si fuera un peaje que hay que pagar por estar en la red y esto de normal no tiene nada, o por lo menos no debería tenerlo. Hay miles de personas en España que diariamente son atacadas en la red y millones en el mundo. Los ciberdelitos se han convertido en una lucha sin cuartel a nivel mundial y en una de las materias prioritarias de seguridad nacional y mundial. Pero hasta la fecha, vamos perdiendo.

El aumento de exposición de las personas en el ciberespacio, algunas de ellas sin experiencia y formación mínima de uso, junto a la presión de las entidades financieras a las personas mayores (y no tan mayores) al uso de internet como único medio de relación con ellas, ha supuesto un incremento brutal en los últimos 2 años de las estafas en internet. Añádale, el teletrabajo y el aumento de las campañas y recursos de los ciber criminales y nos encontraremos ante la tormenta perfecta.

Los delitos asociados con la ciberdelincuencia son muy variados, con una amplia diversidad de agentes y motivaciones. En este sentido, cabe señalar que existe una importante categoría de delitos difíciles de entender desde la lógica de la economía, como el ciberterrorismo o los ataques por motivos ideológicos o de venganza. En estos casos las motivaciones de los ciberdelincuentes están más relacionadas con aspectos psicológicos que con la búsqueda de beneficios económicos.

Los ciberfraudes son cada vez más frecuentes, complejos, destructivos y coercitivos. Tenemos que adaptarnos al nuevo panorama de los ciberataques que están en constante evolución. Los estados requieren ciberdefensas fuertes y resilientes para cumplir tareas críticas, como la defensa colectiva de los ciudadanos indefensos ante esta oleada sin fin, de ataques sin cuartel. La gestión de crisis y la seguridad cooperativa. Los ciudadanos necesitamos estar preparados para defendernos contra la creciente sofisticación de las amenazas y ciberataques a los que todos nos enfrentamos. La Ciber Prevención es de vital importancia para la mitigación de esta tipología delictiva.

La Ciberdelincuencia, se ha convertido en un fenómeno global y multidisciplinar, que requiere la acción conjunta de planes, estrategias y recursos tanto materiales como humanos, para que de una manera eficaz permitan atajar los efectos dañinos que ésta provoca. Uno de los aspectos en los que se debe incidir es la concienciación sobre la implementación en nuestros hábitos cotidianos, de una cultura de la ciberseguridad.

Toda esta nueva forma de proceder por parte de los criminales conlleva a que las Fuerzas y Cuerpos de Seguridad, tengan que estar constantemente alerta para intentar atajar estos fenómenos. Para ello, es necesario la conjunción tanto de una alta preparación como la dotación de herramientas legales y materiales, para llevar a cabo la detección de estos tipos de conductas. Añadiendo, sin lugar a dudas, la tan manida, pero necesaria, y en ocasiones poco utilizada, colaboración público privada.

Abro un tema poco hablado y polémico. Las víctimas de las ciberestafas. Sufren en silencio la tortura intrínseca de ser engañadas, inclusive, son estigmatizadas por esta sociedad llena de "listillos" y lo que es peor, en ocasiones los juzgadores los consideran cooperadores necesarios (imprudencia, dolo eventual, etc.). Además, de que, si ha sido "usado" en una estafa empresarial como gancho, perderá de inmediato su empleo y será tachado de incompetente.

La víctima (dependiendo del caso) sufrirá las tres etapas de victimización. La primera como víctima directa del delito; la segunda como objeto de prueba por parte de los operadores judiciales del Estado en el proceso de investigación; y, la tercera la víctima como sujeto de sufrimiento silencioso en su angustia, estrés, depresión, marginación social al revivir o recordar los sucesos en las cuales se produjo la comisión del delito.

En el caso de ser gancho de un Walling, o de un MINTM, o de un simple Phising, estas incorporan un elemento de ingeniería social al ataque, ya que los empleados sienten la obligación de responder a las solicitudes de una persona que consideran importante o de un proveedor que les pide un cambio de cuenta. Quienes aprovechan la ingeniería social basada en personas para hacerse con lo que necesitan, conocen; explotan y manipulan las emociones humanas para conseguir sus cometidos. Entienden y aplican teorías psicológicas (Teoría de Motivación; de Excitación; de Incentivos y de Opciones, entre otras) para mover sentimientos complejos (compasión; amor; miedo; curiosidad; necesidad de protección o de pertenecer a un grupo) y/o necesidades primarias (sexo; hambre; sueño; sed; etc.) para lograr que los objetivos bajen sus defensas, y entreguen la información que desean sin apenas darse cuenta.

Quienes emplean la ingeniería social basada en las personas saben que los seres humanos compartimos básicamente los mismos miedos, debilidades y necesidades; y estas se reflejan inevitablemente en nuestras interacciones entre pares a través de la web.

Así pues, toman ventajas de las relaciones sociales que establecemos para suplantar la identidad de algún compañero de trabajo; jefe; o alguien representativo para ofrecernos productos o servicios orientados a atacar nuestros activos más preciados.

En definitiva, si además le añadimos que las víctimas de los ataques no tienen un perfil concreto, son de toda raza, credo o religión, entenderemos la magnitud del problema que nos ocupa y el fracaso continuado en su mitigación. En dos palabras. Vamos perdiendo.

Necesitamos con urgencia, voluntad política, para poner freno a esta sangría que como sociedad estamos sufriendo. Y esto no ha hecho nada más que empezar. Medios, formación, legislación adecuada, nuevos organismos de prevención y lucha específica contra el fenómeno, nuevos organismos de ayuda a las víctimas de la ciberestafa. Tan solo así conseguiremos mitigar el fenómeno imparable de los ciberfraudes. ¡Ah! Y mucha "Evangelización". Aunque no te lo creas.

Estafas piramidales

Dinero digital

BITCOIN: ESTAFAS, BLANQUEO DE CAPITALES, BROKERS FALSOS Y OTROS MENESTERES

Jorge Esclapez

Crypto hunter conocido como Deckcard23.

Escanea este QR

Especialista en Análisis Internacional del Cibercrimen y los ciberdelitos relacionados con las criptodivisas y los criptoactivos. Autor del libro "El imperio de bitcoin". Es invitado como referente en prestigiosos blogs relacionados con inversiones, criptodivisas, blockchain y hacking, tan conocidos como el blog de Chema Alonso.

mypublicinbox.com/Deckcard23

La explosión de esquemas piramidales que han aparecido desde que surgiese bitcoin es brutal. A estas alturas me aventuro a afirmar que quien no tiene un conocido tiene un familiar que conoce a un amigo que ha sido estafado.

Todavía hay personas que cuando escuchan hablar de **bitcoin** o **criptomonedas** resuena en su cabeza una palabra: **estafa**. La explosión de **esquemas piramidales** que han aparecido desde que surgiese bitcoin es brutal. A estas alturas me aventuro a afirmar que quien no tiene un conocido tiene un familiar que conoce a un amigo que ha sido estafado. Pero, ¿las criptomonedas son una estafa? ¿cómo sé si me están engañando si quiero invertir? ¿bitcoin no es un arma para el blanqueo de capitales? Las claves a continuación.

¿Son bitcoin y las criptomonedas una estafa?

El dinero digital es una fantástica idea que ha traído consigo muchas ventajas. Gracias a las criptomonedas y a la blockchain, que es la tecnología que las hace posible, la lista de ventajas es interminable y la revolución sin precedentes, aquí unos ejemplos:

- Mayor acceso al dinero (personas del tercer mundo).

- El control del fraude, ya que en todo momento se sabe dónde va a parar el dinero aportado por subvenciones como ejemplo.

- Sistemas de votación sin engaños.

- Productividad, eficiencia y empresas más inteligentes.

- Reducción de costes.

Bitcoin es algo real, pero de origen desconocido y su misión realmente no se conoce, puesto que su creador o creadores están en el anonimato. **Linus Torvalds**, creador del sistema operativo Linux, es el último que se ha añadido a la cada vez más extensa lista de supuestos creadores. Si analizamos el mensaje insertado en el **bloque génesis de bitcoin** podemos deducir que la creación de bitcoin persigue un fin algo anarquista y busca crear un sistema económico donde los bancos y los gobiernos estén al margen.

El primer uso que se le da a bitcoin es en la web oscura para el pago de drogas, armas y cosas ilegales. Al ser un **medio de pago pseudoanónimo** es ideal para aquellos que quieren realizar actos ilícitos. Realmente para saber si las criptomonedas son una estafa deberíamos preguntar a sus creadores. Hay muchísimas criptomonedas que son una estafa y si visitamos la web https://99bitcoins.com/deadcoins/ podemos ver ejemplos de ellas.

Bitcoin y otras criptomonedas son un medio de pago, no son una estafa a menos que sus creadores en el anonimato tengan otras intenciones siendo muy conspiranoicos. Pero sí matizar que en torno a bitcoin y las criptomonedas hay muchas estafas.

¿Cómo puedo detectar una estafa relacionada con las criptomonedas?

El primer consejo para no caer en estafas es simplemente ser un poco curiosos. Me alucina ver como personas que tienen tanto dinero y que contactan conmigo no se han molestado en hacer una pequeña investigación de un **broker**. Aquí os enumero unas herramientas para realizar una pequeña investigación:

- https://www.bitcoinabuse.com/: Comprobar si la dirección bitcoin que nos dan es fraudulenta.

- https://www.blockchain.com/: Ver el dinero que tiene la dirección bitcoin que nos dan, si no tiene nada o muy poco y se observan muchas salidas de capital, es con toda seguridad un fraude.

-https://www.brokeronline.es/5-peores-brokers-scam/brokers-lista-negra/
Lista negra de brokers online.

-https://www.scamadviser.com/
Base de datos de brokers y opiniones

-https://trustscam.es/
Analizador de urls de brokers.

-https://cnmv.es/Portal/Resultado-Busqueda.aspx?tipo=1
Listado de entidades advertidas por la CNMV (Comisión Nacional del Mercado de Valores)

-Buscadores como Google son perfectos para investigar.

El segundo consejo es si es posible invertir por uno mismo utilizando los exchanges y no hacerlo por terceros, ya que es muy posible que pierda su dinero. Hasta la fecha no sé de nadie que invirtiendo en brokers de criptodivisas esté ganando dinero, todo el que me he encontrado me dice que le han estafado, desde 500€ a 300.000€ las cantidades son variables.

Una clasificación sencilla del tipo de estafas en criptodivisas en España sería la siguiente:

1. Físicas: reuniones para captar inversores donde se invita a la víctima. Entre el público hay personas que afirman estar ganando mucho dinero (ganchos). Se recompensa a la víctima por invertir y traer más clientes. Se hace mención a la jubilación y a retornos de la inversión (ROIs) muy altos. Todo va enfocado a convencer a la víctima a que invierta dinero, no lo saquen y traigan más clientes.

2. A distancia: la víctima es contactada por teléfono o redes sociales. Se crea un vínculo de cierta amistad en muchas ocasiones sobre todo cuando está relacionado con aplicaciones de búsqueda de pareja o contactos. Se presenta la plataforma de inversión y empieza el reclutamiento. Se demuestra a la víctima que no hay trampa ni cartón y recibe los beneficios de una pequeña cantidad de prueba invertida (el anzuelo). Por último se quedan con una gran suma invertida, se extorsiona a la víctima para que ingrese más dinero, la amenazan y otras tretas para sacarle más dinero como hacerse pasar por empresas que se lo recuperan.

Blanqueo de capitales en torno a las criptodivisas.

El anonimato que ofrecen algunas criptomonedas ha favorecido el uso de las mismas para el **blanqueo de capitales** y la financiación ilegal. **Monero** es un ejemplo de criptomoneda totalmente anónima, irrastreable, al contrario de bitcoin no puede seguirse su rastro en la **blockchain**. Cualquiera puede crearse una billetera o **wallet** anónima para recibir y enviar criptodivisas lo que hace imposible, a menos que se conozca al propietario por medio de la investigación, identificarla. Se utilizan mulas para mover el dinero entre billeteras o bien convertir el dinero a **moneda fiduciaria** como el euro o el dólar. El crecimiento de cajeros de criptodivisas donde cualquiera con dinero en efectivo puede comprar criptodivisas está fomentando que todo el dinero negro de la economía vaya cambiando de medio. En la web https://coinatmradar.com/ podemos ver los cajeros de criptodivisas que hay en el mundo.

Ya por último concluyo mi análisis con una creencia desde el punto de vista de mi experiencia. Los **exchanges** (actuales bancos 3.0) mientras estén sin regulación y sin una auditoría interna del software que utilizan para las inversiones en criptodivisas son una bomba de relojería. Nadie te garantiza que sean 100% honestos ni hasta qué punto son cómplices tanto en el blanqueo de capitales como en la no protección de los derechos de sus clientes. https://coinmarketcap.com/rankings/exchanges/ (enlace a la lista de referencia de los exchanges a nivel mundial).

Ciberseguridad empresarial

Digitalización

LOS CIBERATAQUES A EJECUTIVOS EXPUESTOS EN REDES SOCIALES

Selva Orejón

Perito judicial especializada en Identidad digital y reputación.

Escanea este QR

Licenciada en Cs. de la Comunicación por la Universitat Ramon Llull y Diplomada en Business Organization and Environment, University of Cambridge. Alma Mater de onBRANDING, empresa con 15 años de trayectoria, especializada en gestión de crisis de reputación online para empresas, instituciones públicas y celebridades.

mypublicinbox.com/selvaorejon

Las personas que conforman una compañía, son el eslabón más importante y a la vez el más débil de la cadena en lo que a ciberseguridad se refiere.

Los ejecutivos de las compañías, blanco fácil para los ciberdelincuentes.

Las personas que conforman una compañía, son el eslabón más importante y a la vez el más débil de la cadena en lo que a ciberseguridad se refiere. Cuando se produce una fuga de información en una empresa nos encontramos con que muchas veces la causa de la fuga tiene un componente social y humano muy relevante.

Más digitales, más inseguros

La pandemia no ha hecho más que agravar esta situación: ha acelerado que seamos más digitales pero también más inseguros.

Es por ello que se hace absolutamente necesario que esta digitalización y automatización de procesos vaya acompañada de una **cultura de la ciberseguridad**. Una cultura que impregne a todos los empleados de una compañía de tal forma que adquieran un espíritu crítico a la hora de navegar por la red, de trabajar en la nube, de detectar un intento de ciberestafa con campañas de phishing cada vez más sofisticadas, etc.

Además, no hay que olvidar que el uso personal que puedan hacer de internet y muy en particular de las redes sociales también pueden acabar teniendo repercusiones negativas en la reputación de sus compañías.

Los ejecutivos de las compañías, blanco fácil para los ciberdelincuentes.

Los ejecutivos, mandos intermedios y altos de las compañías, disponen de poco tiempo y trabajan con mucha presión, lo que afecta a su capacidad de atención. Además, suelen gozar de credenciales que les proporciona acceso a

datos sensibles de la compañía: acceso a cuentas bancarias, programas de nóminas, etc.

La irrupción abrumadora del teletrabajo, y con él el traslado a la nube de documentos y procesos no ha hecho más que agravar la situación.

En el caso de los ataques a ejecutivos, los vectores de ataque favoritos de los ciberdelincuentes son principalmente dos:

Los ataques vía email, phishing: suelen revisar su correo electrónico rápidamente y en ocasiones, sin prestar atención a lo que están descargando o ejecutando, lo que hace que sea más probable que los emails sospechosos pasen desapercibidos.

Los ataques vía navegación: realizar búsquedas en Internet y descargar accidentalmente, o por medio de engaños, códigos maliciosos como Malware, Ransomware, Spyware y cualquier otro tipo de virus con la capacidad de dañar la integridad y acceso de la información.

Ataques de falsificación del correo electrónico: este ataque conocido como ataque del CEO, se caracteriza porque el ciberdelincuente se hace pasar por el director general u otro alto ejecutivo de una organización y envía un correo electrónico para engañar a un empleado para que ejecute transferencias no autorizadas o envíe información confidencial.

Deep fakes y ciberseguridad empresarial

Su creciente capacidad de los Deep fakes para suplantar a personas con éxito, tanto en audio como en vídeo, está haciendo que los ciberdelincuentes estén cada vez más interesados en ellas para atacar y estafar a empresas e instituciones públicas.

"Nosotros ya hemos tratado casos de este tipo, del conocido como **fraude del CEO**, mediante Deep fakes de audios. El consejero delegado de una empresa nos llamó preocupado porque le habían tenido al teléfono durante un minuto y medio mediante ingeniería social sin decirle concretamente para qué, y temía que fuese para conseguir su voz y, mediante concatenaciones, poder reproducirla y usarla para tratar de cometer un fraude contra la compañía", explica **Selva Orejón**, experta en ciberseguridad e identidad digital de **onBRANDING**.

3 claves que permiten a los ejecutivos ciberprotegerse y ciberproteger a su empresa.

Rastrear y detectar si se ha producido en la red algún tipo de filtración de información o datos que sean sensibles para la compañía. Debemos adquirir una actitud proactiva en este aspecto, es importante que seamos capaces de identificar las amenazas antes de que los ciberdelincuentes lo hagan, de esta forma podremos reducir las probabilidades de sufrir un ciberataque.

Existen herramientas que permiten hacer este rastreo para detectar fugas de información y vulnerabilidades como las siguientes:

Registro de dominios similares: amenaza de phishing, abuso de marca y ciberocupación.

Credenciales de empleados filtradas

Subdominios expuestos

Aplicaciones móviles deshonestas

Documentos filtrados

Código fuente filtrado

Secuestro de dominio

Caducidad de certificado SSL y del dominio

Profiling de candidatos: cuando se contrata a alguien en una compañía, no solo se está reclutando a empleados, sino que se está seleccionando a personas que van a representar a la compañía fuera de ella. Muy especialmente si se trata de puestos directivos. Opiniones en foros o redes sociales, fotografías o contenido audiovisual sensible, delitos omitidos, etc. En definitiva se trata de buscar información y cualquier tipo de contenido en los medios digitales que puedan representar una amenaza reputacional para la compañía contratante.

Desposicionar o eliminar el contenido sensible: con el fin de reducir la exposición al riesgo reputacional, de pérdida de privacidad o seguridad para la compañía, sus marcas y sus líderes debe eliminar aquellos enlaces de contenidos de redes sociales, buscadores, etc.

Indagación

Paginas web

Datos en Internet

¿QUÉ SABE LA CLEARWEB, DEEPWEB Y DARKNET DE NOSOTROS?

Jorge Coronado

CTO en Lazarus Group Technology y CEO en Quantika14

Escanea este QR

Fundador de Happy Hacking Sevilla, la comunidad con más actividad en Sevilla sobre Ciberseguridad. Co-organizador del congreso de OSINT y Ciberinteligencia "OSINTCITY". Co-autor del Primer Protocolo Institucional en España ante la violencia de género en las redes sociales en Andalucía y autor del Protocolo de actuación para la búsqueda de personas desaparecidas a través de las TICs.

mypublicinbox.com/JorgeWebsec

El contenido web que podemos encontrar a través de los buscadores más conocidos se podría llamar Web o ClearWeb. La Deep Web son las páginas que no son fácilmente encontradas por los buscadores normales. Y la DarkWeb son las páginas que usan medidas para evitar ser localizadas o que restringen su acceso a un grupo concreto de personas.

La palabra inglesa "WEB" viene de World Wide Web, un sistema de documentos (páginas web) interconectados por enlaces a través de Internet. Y "deep" viene de profundo. Es decir, son páginas web ocultas en la profundidad – y, por ende, más difíciles de encontrar.

Vamos a intentar explicarlo de otra forma más sencilla.

El contenido web que podemos encontrar a través de los buscadores más conocidos se podría llamar Web o ClearWeb. La Deep Web son las páginas que no son fácilmente encontradas por los buscadores normales. Y la DarkWeb son las páginas que usan medidas para evitar ser localizadas o que restringen su acceso a un grupo concreto de personas.

Digamos que la ClearWeb – las páginas webs indexadas por los buscadores habituales – es el centro de Sevilla; los bares buenos de barrio donde se pueden comer los platos tradicionales y que no aparecen en Tripadvisor son la DeepWeb; y el bar en el que, para entrar, debes conocer un código secreto en la puerta es la DarkWeb.

Evidentemente, este último sitio es el que muchos delincuentes utilizan para comunicarse o vender sus productos y servicios; aunque podríamos decir que la DeepWeb – el bar de barrio – también es un entorno propicio para muchos ciberdelincuentes.

Por ello, tanto a empresas como a particulares les interesa saber si sus datos aparecen por estos lugares. Su monitorización no es sencilla. Entrar en foros como un foráneo no es buena idea y muchos cuerpos de seguridad y agencias de inteligencia tienen agentes encubiertos durante meses e incluso años. Estos informan de qué objetivos o víctimas van apuntando con sus mirillas los ciberdelincuentes.

De igual manera que los cuerpos de seguridad y agentes de inteligencia, los peritos informáticos realizamos un trabajo de certificación e indagación para directivas de empresas, famosos y cualquier persona que pueda pagar estos servicios.

Soy Jorge Coronado, trabajo junto a mi equipo como perito informático, y en este artículo me gustaría enseñaros cómo auditar si nuestros datos están en Internet, ya sea en la DeepWeb, Darknet o Clearweb.

Monitorizar la ClearWeb

Controlar la información que tiene de nosotros Google, Bing y las redes sociales son tareas tediosas pero nada técnicas. Solo requiere que el usuario realice los siguientes pasos:

LO PRIMERO será averiguar qué sabe Google de nosotros o de nuestra empresa usando DORKs. Para ello, escribe en el buscador lo siguiente:

Intext:nombre+apellidos
intext:nombre de la empresa

Intext:"TU DNI"

Inurl:"tu username"

Tras hacer un egosurfing vamos a configurar la aplicación gratuita de Google Alert con nuestros datos: nombres, teléfonos, etc. No obstante, el servicio no es tan bueno como aparenta y recomiendo realizar la tarea anterior manualmente.

LO SEGUNDO es un v y un método que aprendí buscando a una persona que había borrado gran parte de su huella en Internet: no todo está en Google. Es necesario buscar nuestros nombres en Bing y DuckDuckGo.

LO TERCERO es la más importante porque la mayoría de nuestros datos los volcamos en las redes sociales. Cada una de ellas tendrá un método diferente, pero por ley deben proporcionarnos descargas de todos los datos que tienen sobre nosotros. Mi consejo es que, si no usas una cuenta, la des de baja o la elimines.

LO CUARTO será encontrar nuestras fotos por Internet. Podemos usar buscadores de imágenes inversas: Yandex, Tineyes y Google. También podemos usar el reconocimiento facial, tecnología que debemos manejar con precaución porque estos servicios suelen ser de pago y hay que vigilar que no estemos regalando nuestra cara para que el machine learning siga aprendiendo. Es decir, tu cara servirá para mejorar el algoritmo y quedará almacenada en servidores de empresas o gobiernos con unos intereses que desconocemos.

LO QUINTO y último de este apartado, será para las personas un poco más técnicas. Podrán usar Pystemon y tener su propio sistema de monitorización. Entre ellas, la conocida plataforma de Pastebin.

¿Y la DeepWeb y DarkNet?

TOR es la red más conocida de la Deep Web. En ella también hay páginas de la Darknet. Foros y plataformas poco accesibles son un nido perfecto para cibercriminales. Muchas de estas exponen su producto (base de datos y empresas que han sufrido una intrusión) como reclamo para una recompensa o pago por el secuestro.

Existen buscadores de la DeepWeb, pero duran poco tiempo. Por ejemplo: darcksearch.io que actualmente se encuentra cerrada al público.

TOR no es toda la Deep Web y mucho menos la DarkNet. No obstante, es la más conocida y si queremos monitorizarla deberemos usar técnicas avanzadas muy lejos de un usuario medio.

Sin embargo, existe Dante's Gates, un bot de Telegram que permite a los usuarios y empresas realizar todo este trabajo en muy poco tiempo. Sus comandos /buscarpersona y /buscartelefono permiten a los usuarios saber qué información puede haber en Internet sobre ellos. Además, también dispone de un buscador de usernames. Utiliza diferentes APIs y una tecnología propia para identificar los datos asociados a las identidades que le digamos. Una persona puede tener varias identidades en Internet y un nombre varias personas asociadas y viceversa.

Lo bueno de esta aplicación es que en pocos minutos habrá realizado todos los pasos que hemos comentado anteriormente y tendremos un informe con los resultados en PDF.

Como conclusión, quiero dejar claro que no existe un superhéroe como Batman que tenga oídos y ojos en todo Internet. Sin embargo, es responsabilidad nuestra invertir y preocuparnos por nuestros datos. Tendremos que usar diferentes aplicaciones y soluciones. Y no pienses que por no haber subido nada a Internet, no sabe nada de ti.

Riesgos en la web

Mundos virtuales

CIBERAMENAZAS EMERGENTES EN LOS ENTORNOS DEL METAVERSO

Yaiza Rubio

Chief Metaverso Officer Telefónica.

Escanea este QR

Responsable del proyecto de "Network Tokenization. En 2021 lideró el proyecto de Smart WiFi y trabajó como Analista de ciberinteligencia para ElevenPaths, la Unidad de Ciberseguridad de Telefónica. La primera mujer hacker española en realizar ponencias en eventos como DEF CON y Black Hat Briefings. Autora de BitCoin: La tecnología Blockchain y su investigación y el "Manual de investigación en fuentes abiertas (OSINT)".

mypublicinbox.com/yrubiosec

"Ya los mundos virtuales tienen millones de usuarios conectados diariamente. Es, en este sentido, donde se torna todavía más relevante trabajar sobre la identidad, la privacidad y la seguridad de las personas."

En la historia de la revolución digital existen unos cuantos inventos que han hecho cambiar la forma que tenía la gente de ver el mundo. Es este mismo instante, debido a la pandemia, el asentamiento de tecnologías como la realidad virtual o la web3.0, además de su aceptación por parte de la Generación Z, nos hace pensar que estamos muy cerca de hacer realidad ciertas visiones que se tienen del Metaverso.

Ya los mundos virtuales tienen millones de usuarios conectados diariamente. Es, en este sentido, donde se torna todavía más relevante trabajar sobre la identidad, la privacidad y la seguridad de las personas. Empresas como Meta, que se encuentra desarrollando la plataforma de Oculus, necesitan de perfiles[1] que comprendan los riesgos a los que se puede enfrentar la compañía, ya que en este nuevo entorno las amenazas se pueden manifestar de múltiples maneras y podrían afectar a miles de millones de personas.

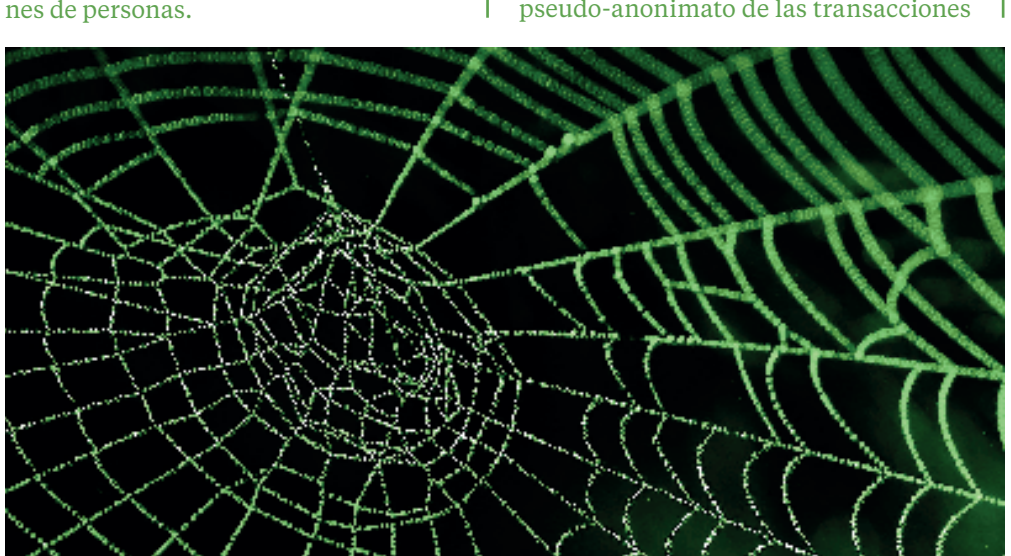
Recuerdo la primera conferencia que impartí de seguridad con mi compañero **Félix Brezo**. Fue en 2015. En la RootedCON y trataba sobre seguridad en Bitcoin. De aquella, había mucho desconocimiento sobre su funcionamiento y nuestro único interés era entender la tecnología con el objetivo de conocer las limitaciones de seguridad. Llegamos a profundizar en uno de los grandes retos que tiene actualmente la web3.0: la generación de los wallets y el almacenamiento de las claves privadas por parte de los usuarios.

Hicimos un experimento que consistía en generar wallets a partir de palabras. No nos podíamos creer que ese tipo de funcionalidades pudieran existir aunque para el usuario final fuera una forma sencilla de generar su wallet en el caso de pérdida. Así que generamos un diccionario, generamos los wallets pertinentes y llegamos a validar que ese procedimiento tan inseguro era usado por cientos de usuarios de Bitcoin. Años después, ese aprendizaje nos sirvió para comprender el riesgo al que se someten los usuarios con la gestión de sus wallets, así como, ya con la aparición de wallets como Metamask o Ronin, comprender cómo se comunican con las dApps y los potenciales riesgos que existen cuando se otorgan ciertos permisos.

Asimismo, en 2017, Félix y yo presentamos en EuskalHack una idea que no nos parecía para nada muy descabellada. Nunca hemos sido analistas de malware, pero conocíamos las principales propiedades que tiene una cadena de bloques, por lo que no nos parecía que fuera a tardar mucho la aparición de aplicaciones maliciosas cuyo C&C se sirviera de la infraestructura de esta tecnología de cara a que los nodos infectados siempre tuvieran de forma permanente dónde acudir para recibir las órdenes a ejecutar. Años después, no nos sorprendió la aparición de familias de malware como el ransomware Cerber y su manera de coordinarse con los nodos infectados.

Y, por último, otra de las investigaciones que nos hizo reflexionar sobre esta tecnología fue durante el incidente de Wannacry. Apenas unos días después de que se cerraran las ediciones de 2017 de Blackhat USA y Defcon, el 3 de agosto se produjeron los primeros movimientos desde las direcciones del cibercriminal. Así es como comenzaba un proceso de "persecución" digital donde pocos cayeron en la cuenta de la importancia de un evento para el ecosistema de Bitcoin: el hard fork de Bitcoin Cash. Los analistas que por aquel entonces estábamos pendientes, nos dimos cuenta de que el siete de noviembre de 2017, los autores realizaron una única transacción en la que juntaron todo el saldo en Bitcoin Cash. Este tipo de experiencias nos ayudó a aprender sobre el anonimato o pseudo-anonimato de las transacciones y, por consiguiente, sobre el concepto de fungibilidad donde todas las monedas no tiene porqué valer lo mismo si previamente, por ejemplo, han estado relacionadas con el cibercrimen. ¿Acaso aceptarías a precio de mercado un pago con monedas procedentes de algún tipo de extorsión?

La seguridad es una forma de aproximarse a la tecnología. Para saber cómo hackearla previamente se tiene que haber interiorizado sus fundamentos. Todo este tiempo nos ha servido para aprender sobre unos riesgos existentes en web1.0 y web2.0. Sin embargo, muchos a los que nos someteremos en el entorno del Metaverso ni siquiera somos todavía conscientes. No tengo ninguna duda que los security researchers tendrán un papel relevante ayudándonos a crear estos nuevos mundos donde prevalezca la seguridad y la privacidad desde el diseño.



Principios éticos

Vurnerabilidad en la Red

HACKING ÉTICO ¿POR QUÉ ES IMPORTANTE PARA LAS EMPRESAS Y LA SOCIEDAD?

Pablo González

Responsable del equipo de Ideas-Locas en CDO en Telefónica.

Escanea este QR

Es MVP de Microsoft desde 2017. Es fundador de hackersClub, Co-fundador del blog de seguridad informática Flu Project y Autor de diferentes libros de la editorial 0xword: Metasploit para Pentesters, Ethical Hacking o Got Root, entre otros. Además, de Speaker en diferentes congresos internacionales de Ciberseguridad.

mypublicinbox.com/PabloGonzalez

Las empresas necesitan medir cómo de eficaces están siendo sus inversiones en seguridad. El hacking ético es una herramienta que permite obtener dicha información y dota a la empresa de datos para la toma de decisiones.

El hacking es hacking. El hacking es pasión, inquietud, conocimiento, no conformarse. El hacking es lo que queremos para los jóvenes: que no se conformen, que no pierdan el interés por cómo funciona el sistema, sea cual sea éste, que quieran conocer, que tengan pasión por el conocimiento. El hacking es un motor.

Desde hace muchos años le añadimos la palabra ético para indicar que los conocimientos serán utilizados para hacer el bien, para ayudar, para mejorar. Si los conocimientos se utilizasen para hacer el mal, no hablaríamos de hacking, hablaríamos de delincuencia, sin más.

Las empresas necesitan medir cómo de eficientes y eficaces son sus controles de seguridad, por ello aplican diferentes herramientas y procesos. Hay que entender que las empresas necesitan conocer si deben invertir más en seguridad, mejorar lo que tienen o, directamente, implementar soluciones que no disponen. La seguridad es un proceso cíclico en el que se debe tener en cuenta que la tecnología avanza rápido, muy rápido. Debido a esto, las vulnerabilidades, las amenazas, los riesgos evolucionan, aparecen y ponen en jaque a muchas organizaciones. Gracias a la gestión de la seguridad en las organizaciones se puede ir controlando todo lo referente a estos riesgos que amenazan a las empresas.

Dentro de esta gestión se utilizan diferentes herramientas. Una de estas herramientas es el hacking ético. El hacking ético es el conjunto de pruebas que permitirá evaluar la seguridad en diferentes aspectos y entornos de la organización. Las pruebas varían mucho dentro del hacking ético, pero todas tienen en común la identificación de aspectos que están fallando dentro de la organización y que dichos fallos pueden provocar que un atacante pueda aprovecharse y sacar un beneficio.

Para muchos lectores, el hacking ético puede ser una película dónde hay un bando que son los buenos y un bando que son los malos, los cuales son simulados por los profesionales del sector. En realidad, ambos bandos están en el mismo equipo en el de llevar a cabo sus acciones con el objetivo de proteger la información de la empresa. Es más, la parte defensiva y la parte ofensiva trabajarán juntas en algún momento para mejorar la seguridad de la organización.

¿Y qué pruebas se hacen en esta "película"? Las pruebas son muy diferentes. ¿Auditorías? ¿Pentesting o test de intrusión? ¿Pruebas de concienciación? ¿Simulación DDoS? ¿Simulación de una fuga de información? Sí, la verdad es que las pruebas son muy diferentes, pero, ¿Qué son estas pruebas? Lo primero es que el hacking ético y sus pruebas son algo dinámico, ya que dependerá de la tecnología emergente, de las amenazas nuevas, de los riesgos asociados que van apareciendo a los nuevos sistemas de los que consta la infraestructura de una organización.

Las auditorías pretenden identificar el máximo de vulnerabilidades sobre sistemas fundamentales para que la organización lleve a cabo su actividad. Por ejemplo, una auditoría sobre los recursos web de la empresa permite obtener información sobre el estado de éstos, permitiendo tomar decisiones sobre las mejoras o inversiones que se necesitan. Las auditorías se llevan a cabo sobre diferentes ámbitos: las páginas web, los servicios internos, el servidor de correo electrónico, sobre cualquier servicio que sea importante para la actividad de la organización.

El test de intrusión es una simulación de un ataque para verificar que la empresa tiene las medidas adecuadas para lograr evitar dicho ataque. El objetivo es alcanzar unos elementos que se marcan a priori. Si el pentester tiene éxito, la empresa entenderá que tiene caminos por los que un atacante pueda alcanzar datos importantes y hacer un gran daño. Como se puede entender, este tipo de pruebas aportan un gran valor a la organización.

La prueba de concienciación permite probar cuál es el nivel de conocimiento de los empleados ante una amenaza que se vuelve "real". La empresa quiere validar si sus empleados están concienciados y conocen las políticas internas de seguridad para detectar y actuar en caso de una amenaza. ¿Qué ocurre con los empleados que caen en este tipo de pruebas? Realmente, podrían poner en riesgo la seguridad de la organización, por lo que deben pasar por charlas y formaciones dónde se les explique qué deben hacer ante ciertas situaciones.

Y como si llegásemos al final de la película de la tarde, tenemos el producto de todo el trabajo técnico: el informe. La visión de cómo está la organización. De lo que necesita la organización. Es algo fundamental. Es algo sobre lo que los profesionales ponen el "mimo" adecuado, ya que es la presentación de su trabajo. El trabajo realizado que permitirá a la organización tomar decisiones sobre el camino que deben llevar en esto llamado: ciberseguridad.

Privacidad
Ciberseguridad
Conferencias

CONFERENCIAS (CONS) HACKERS

Gabriel Bergel

CEO y Cofundador de 8.8 Computer Security Conference

Escanea este QR

Miembro del Directorio Global de (ISC)², Associate Partner, Security & Resilience Consulting Services en Kyndryl, Coordinador del Centro de Ciberseguridad Industrial (CCI), Director de Políticas Públicas en Whilolab y conductor de #8punto8 en www.radiodemente.cl (1er programa radial de Ciberseguridad en Chile). Cuenta con 20 años de experiencia en distintos rubros de seguridad de la información.

mypublicinbox.com/Ragnar

Imagínense lo que es una "conferencia hacker", sería como la reunión de estas personas "extrañas", curiosas, extravagantes, que llaman mucho la atención, la verdad es que eso y mucho más, les contaré mi experiencia personal.

Definitivamente, la palabra y el concepto "Hacker" genera mucha curiosidad y llama la atención, lamentablemente, muchas veces de una manera negativa, no me detendré en este punto, hay innumerables artículos y hasta una campaña donde trabajamos en aclarar el término hacker, con el cual nos referimos a un "investigador", un apasionado de la tecnología, que puede invertir muchas horas en entender cómo funciona y cómo podría funcionar si pensamos "fuera de la caja", ¿que vulnerabilidades podría tener? ¿como podría exponer a la gente o violar nuestra privacidad? etc. Todo lo anterior con el único objetivo de mejorar la tecnología y proteger a las personas.

Imagínense lo que es una "conferencia hacker", sería como la reunión de estas personas "extrañas", curiosas, extravagantes, que llaman mucho la atención, la verdad es que eso y mucho más, les contaré mi experiencia personal.

Desde la universidad que alucinaba con los "hackers", sobre todo después de ver la película el año 1996 o 1997 no lo recuerdo bien. Fue el 2003 cuándo comencé a trabajar de manera profesional en la materia, empecé a asistir a conferencias de ciberseguridad, pero eran todas comerciales, metían mucho miedo y luego te vendían una tecnología que solucionaba todo. Habían otras conferencias también, pero más relacionadas con cumplimiento de normativas o gestión de riesgos.

Yo particularmente estaba aburrido de ese tipo de conferencias. Por varios años traté de ir a la Ekoparty en Buenos Aires, Argentina, pero por diferentes razones no había podido ir; lo mismo con Defcon, varios amigos, sobre todo argentinos me hacían bromas por lo mismo. En Chile, tampoco habían conferencias hackers, solo reuniones y súper under, hasta que llegó el 2011, año muy especial para mí en este ámbito, ya que fue el año que creamos la 8.8, nuestra conferencia Hacker, titulada "Hacker unidos jamás serán vencidos".

Nunca pensamos que cumpliríamos 12 años haciendo la conferencia y no solo en Chile, sino en varios países más. Esa 1.ª versión fue una odisea, pero sentíamos que era muy necesario, ya que no existía una instancia como esta, una reunión donde pudiéramos juntarnos a hablar, aprender, compartir información técnica y un ambiente distendido y además tomando cerveza (gratis).

El 2011 fue especial también porque pude asistir a mi 1.ª conferencia Hacker internacional que fue la Ekoparty 2011, que era la versión 7.ª de la conferencia, recuerdo que tenía un estilo ruso que me encantó y me marcó. Además, en esa conferencia conocí a Chema Alonso, hoy día mi amigo, con quien tuve la suerte de trabajar y seguir trabajando, ya que es Director de 8.8.

Hoy llevo asistiendo y dando charlas en conferencias desde esa fecha, he tenido la oportunidad de dar charla en muchas partes del mundo, las que más recuerdo son en Rusia en PHDays 7 donde asisten más de 6000 personas y en la Villa de Biohacking en Defcon 26 en las Vegas donde asistieron más de 20.000 personas. Vale la pena mencionar que Defcon es la conferencia más grande e importante, junto con Chaos Communication Congress en Alemania.

¿Qué es una conferencia Hacker?

Es todo lo que imaginan y mucho más, es una reunión de hackers donde principalmente se comparte conocimiento, experiencias, se conoce gente del rubro y se pasa bien.

Principalmente, las conferencias hackers tienen uno o varios tracks de charlas, siempre son conferencias de seguridad informática, charlas técnicas, no relacionadas con gestión, gobernanza o estrategia, al contrario, directo a bit y al byte, muchas veces incluso no se entienden porque son muy técnicas o específicas, siempre entregando el estado del arte en la materia. Aquí tenemos la opción de seleccionar las charlas de nuestra preferencia y asistir a ellas, siempre hay espacios para stands de patrocinadores, donde te informan de que trata su empresa, servicio, plataformas y te regalan merchandising. Las conferencias más grandes, como Defcon, tienen villas que son como "mini" conferencias dentro de la conferencia principal, donde se trata un tema en particular, y podemos encontrar la Villa de "Ingeniería Social", de "IoT", "La de hackear Autos" entre otras. Dado que es como una peregrinación (llevo 7 años asistiendo a Defcon de manera ininterrumpida), siempre las conferencias están rodeadas de fiestas y otras actividades extra programáticas organizadas de manera espontánea, de manera independiente o por patrocinadores. Además, estas instancias sirven para hacer muchas reuniones, si además sumamos que la ciudad donde se realiza la conferencia es nueva para ti, sumas todas las actividades de turismo.

Recomiendo absolutamente la asistencia a este tipo de conferencias, me imagino que todas las conferencias, independiente del rubro, sirven para lo mismo, reunirse con amigos, colegas, compartir conocimiento, aprender lo nuevo, actualizar conocimientos, hacer crecer la red de contactos, fundamental hoy en cualquier rubro, conocer gente nueva, compartir unas cervezas, ir de fiesta, conocer lugares nuevos. Yo, personalmente, crecí mucho como profesional asistiendo a conferencias hackers, y pienso que cada vez nos debería costar menos pedir permiso en el trabajo o al contrario, que el trabajo debería cubrir los gastos para asistir a este tipo de conferencias, porque están capacitando a su personal técnico, lo están actualizando. Hoy en día, con lo rápido que sucede todo, es fundamental.

¿Lo recomiendo? Totalmente, de hecho este año se cumplen 30 años de Defcon (11 al 14 de agosto), 22 años de Ekoparty y 12 años de 8.8 (8.8 Real, el 20 y 21 de octubre), por ende, espero verlos en alguna de estas instancias.

Seguridad Informática
Ciberseguridad

DE PROFESIÓN: HACKER

Chema Alonso

Chief Digital Officer en Telefónica.

Escanea este QR

Reconocido hacker español, miembro del Comité Ejecutivo de Telefónica, que ocupó varios roles en la multinacional desde 2019, y actualmente como Chief Digital Officer es responsable de Innovación, Datos, Plataformas, Productos y Servicios Digitales. Emprendedor y apasionado de la tecnología tiene un perfil muy mediático gracias a su intensa actividad como divulgador.

mypublicinbox.com/ChemaAlonso

"Y mi vida se hizo más divertida. No porque dejara la programación, las estructuras de datos, la algorítmica, las bases de datos o la geometría computacional. Ni mucho menos. Si no porque en el mundo del hacking todo eso que me gustaba se sigue utilizando, pero a otro nivel. Y porque lo que más engrandece a uno de esos hackers míticos es que son capaces de poner a jugar juntas todas las disciplinas tecnológicas. Y me dio todo en mi vida profesional."

Nunca pensé, ni remotamente, en dedicar mi vida a la seguridad informática, al hacking, a la ciberseguridad. Ni remotamente. A mí me gustaba programar. A mí me gustaba la algorítmica, las estructuras de datos, las bases de datos, la geometría computacional. Ni se me pasó por la cabeza hacer la asignatura de Seguridad Informática cuando era estudiante en la Universidad Politécnica de Madrid. Era una asignatura optativa, y yo opté por no hacerla. Cuestión de elegir lo que a uno le gusta.

Pero con el tiempo la cosa cambió. Comencé a trabajar y descubrí el gusto por las técnicas de hacking, por hacer cosas que pensaba que no se podían hacer. Por desarrollar técnicas, y crear proyectos que tuvieran que ver con la seguridad informática, con el hacking, con la ciberseguridad. Y mi vida se hizo más divertida. No porque dejara la programación, las estructuras de datos, la algorítmica, las bases de datos o la geometría computacional. Ni mucho menos. Si no porque en el mundo del hacking todo eso que me gustaba se sigue utilizando, pero a otro nivel. Y porque lo que más engrandece a uno de esos hackers míticos es que son capaces de poner a jugar juntas todas las disciplinas tecnológicas.

Y me dio todo en mi vida profesional.

Dedicarme al hacking, la seguridad informática, la ciberseguridad, ha hecho que, lo que antaño fuera denostado, repudiado y casi perseguido, se convirtiera en un activo más que valioso en mi carrera profesional. Vivir con el espíritu de los hackers, de hacer cosas, de pensar en siempre llevar la tecnología un paso más allá de lo que se piensa. Solo un pasito más. Un milímetro más. Me mantiene vivo, activo, inquieto, y enganchado a mi trabajo. Me hace feliz, y gracias a eso, dedico más tiempo a eso que me hace feliz, y me ayuda a ser mejor profesional.

Yo he tenido la suerte de poder crecer casi al mismo tiempo que esta profesión. He visto cómo el trabajar en seguridad informática, en seguridad de la información, en hacking o en ciberseguridad se ha ido profesionalizando con una miríada de roles claramente definidos que casi permite que, cualquier persona, tenga su cabida en uno de estos roles. El universo de profesiones alrededor de éste, otrora residual, rincón de la tecnología, abre una plétora de oportunidades para trabajar "De hacker". Pero.... No todas son iguales, ni todas necesitan los mismos perfiles personales, ni las mismas habilidades, ni las mismas capacidades.

Es decir, una persona creativa puede ser un gran Red Teamer, o un gran Pentester, e incluso un gran Bounty Hunter, pero para ser un buen QA de Seguridad, un Blue Teamer o trabajar en un SOC como ingeniero de escalación, puede que su creatividad sea menos valorada en función de alguien más metódico, minucioso y detallista. Y por supuesto, nada tiene que ver con trabajar en el equipo del CERT, en el equipo del CISO, del DPO, donde hacen falta dotes de planificación, negociación y comunicación. Y si ya estás en el CSIRT y toca meterse en la WarRoom en una crisis, más vale que traigas nervios de acero y una

buena capacidad de gestionar la presión y tomar decisiones acertadas con poco tiempo.

Seguro que si no eres de nuestro gremio te he podido dejar un poco perdido con tanto acrónimo y nombre técnico en inglés que no has sido capaz de entender. No te preocupes. Es normal si no has vivido como muchos de nosotros el nacimiento y creación de esta profesión y todas sus ramificaciones. Hoy en día, como te dije al principio, es una profesión muy madura con mucha clarificación de funciones, capacidades y habilidades necesarias. Y para tu información, son muchas más de las que he citado en esa lista.

Ahora bien, la gran pregunta que se deben hacer los que quieren trabajar en este mundo es, "¿y cómo sé yo a lo que me quiero dedicar?" "¿cómo saber qué es lo que me va a gustar más y en lo que voy a ser mejor?" Sabia pregunta que en mi época se resolvía mediante el viejo mecanismo empírico de ensayo y error. O probar y probar hasta tu sitio encontrar.

Lo cierto es que, hoy en día, la cosa es distinta, y con una aproximación tecnológica también se puede saber qué profesión de seguridad informática, hacking o ciberseguridad se te va a dar mejor. O lo que es lo mismo, en qué profesión de este mundo laboral tan prolífico de roles en ciberseguridad tus capacidades personales, las que tienen que ver con tus habilidades más intrínsecas a ti como son la creatividad, la gestión de la comunicación, la presión, el pensamiento lateral, el razonamiento computacional, la atención, las habilidades de empatía, liderazgo, lógica o desempeño, por citar algunas, encajan más.

Para eso creamos **Singularity Hackers**, una plataforma que te ayuda a reducir la incertidumbre y el número de errores a la hora de querer ser "hacker"o trabajar en este mundo laboral.

La idea es muy sencilla, la plataforma en https://singularity-hackers.com (https://singularity-hackers.com/?rid=UvzX4r-FC-b_QrcU-T16RnCX1wiMRx2XWDfIN-Hukcs48) evalúa a cada una de las personas que quieren descubrir cuáles son los roles profesionales en los que más encaja con varios test de habilidades, pruebas de capacidades y evaluación de características personales, durante varias horas. Una vez terminados, la persona es mapeada en un rango único en la plataforma, y se buscan las tres profesiones en ciberseguridad – de entre unas cincuenta disciplinas profesionales y roles laborales distintos – en las que las cualidades y habilidades de esa persona encajan más, haciendo que esté preparado para brillar en esa profesión de manera natural. Es decir, su forma de ser encaja perfectamente con esa profesión.

Por supuesto, eso no quiere decir que esté listo para desempeñar ese trabajo profesional, sino que, con mucha probabilidad, si se forma para alguna de esas profesiones, su disposición natural hará que encaje en ellas, ya que las cualidades que se valoran en ellas son justo las que tiene. Es decir, con modelos de Inteligencia Artificial y usando tecnología creamos una plataforma en la que te ayudamos a saber qué tipo de hacker llevas dentro. No me digas que no es muy hacker hacer algo así.

"Nunca hubo guerra buena ni paz mala."
— Benjamin Franklin