



Caja de herramientas del experto en ciberseguridad

Raquel Puebla González
(Entelgy Innotec Security)

Leandro Martínez Peñas
(Universidad Rey Juan Carlos)

Erika Prado Rubio
(Universidad Rey Juan Carlos)

Un suplemento para
Karma Zero



Caja de herramientas del experto en ciberseguridad

Autor: Raquel Puebla González; Leandro Martínez Peñas,
Erika Prado Rubio

Diseño de cubierta y fondos de página: Erika Prado Rubio.

Ilustraciones: Mónica Peñalver

ISBN: 978-84-09-29918-8.

Edita: Asociación Veritas para el Estudio de la Historia, el
Derecho y las Instituciones.

Junio, 2021.

La realización de la presente publicación ha sido financiada por el Ministerio de Defensa, a través de la Convocatoria de Ayudas para promover la Cultura de Defensa 2021, formando parte de las actividades del Proyecto “Todos contra nosotros, nosotros contra todos: desarrollo e implementación de modelos gamificados competitivos para la difusión de la Cultura de Defensa”.

Para su realización se ha contado con la colaboración de Entelgy Innotec Security, a través de las aportaciones y revisiones realizadas por los especialistas de su plantilla, sin cuya labor esta publicación no hubiera podido realizarse.



ÍNDICE

Presentación.....	7
Veinte buenas prácticas para evitar ser víctima de un ciberdelito	11
Parte I: Panorama de ciberseguridad actual	
- Capítulo I: conceptos básicos de ciberseguridad.....	17
1.- Origen de la ciberseguridad.	17
2.- Amenazas principales a la seguridad informática.....	20
- Capítulo II: Cronología y evolución de los principales ciberataques de la Historia.	45
1.- Precedentes: el caso Blanc y los trabajos de Turing. ...	45
2.- Los primeros ciberataques.	50
3.- La eclosión de los ciberataques.....	53
4.- Stuxnet.	55
5.- Entre Stuxnet y Wannacry	57
6.- WannaCry.	65
7.- NotPetya.....	69
- Capítulo III: Formas de luchas contra las amenazas a la seguridad informática.	73
1.- Legislación supranacional.....	73

2.- Legislación en España.....	76
- Capítulo IV: Bibliografía.....	87

PARTE II: AYUDAS DE JUEGO

- Capítulo V: Consejos para usar ciberseguridad en <i>Karma</i>.	107
1.- Antes que nada: que no cunda el pánico.	107
2.- Consejos variados.	112
3.- Resolución de acciones.	117
- Capítulo VI: Ayudas para personajes	123
1.- Rasgos	123
2.- Uso de Especialidades genéricas de ciberseguridad .	132
3.- Especialidades de ciberseguridad.	133
4.- Personajes	138
- Capítulo VII: Acciones de ataque y defensa	159
1.- Tipos de acciones agresivas	159
2.- Acciones defensivas.....	171
3.- Protecciones.....	174
- Capítulo VIII: Glosario	189
- Licencia de uso.....	201

PRESENTACIÓN

Saludos, viejo o nuevo amigo de *Karma*. Siempre es una alegría verte por aquí. Antes de tratar de encontrar las vulnerabilidades en la red informática de una malvada empresa multinacional, antes de hacer danzar tus dedos sobre el teclado mientras las columnas de código se reflejan con una luz verdosa en las lentes de tus gafas, antes de tratar de sustraer un token repleto de claves criptográficas del maletín de un agente enemigo en un bazar de Oriente Medio, concédenos unos instantes.

Caja de herramientas para el especialista en ciberseguridad es un suplemento para el sistema *Karma*. Por tanto, necesita del reglamento básico, *Karma Zero* para que puedan jugarse aventuras incluyendo los elementos que ofrece. Si no lo tienes, no te preocupes, puedes descargarlo en formato pdf, de forma completamente libre y gratuita, en la página web de *Karma*. Aquí te dejamos el link:

<https://karmajuegoderol.com/>

De la misma forma, si prefieres otros sistemas, adaptar algunos de los contenidos aquí incluidos sin duda te será fácil. Lo importante es que lo juegues y, más aún, que no olvides algunos de los consejos que incluye.

Caja de herramientas para el especialista en ciberseguridad es un suplemento muy especial, ya que para su elaboración hemos contado

con Raquel Puebla González, especialista en ciberseguridad que nos ha brindado su amplia experiencia y sus muchos conocimientos para poder ofrecerlos, en la primera parte de este módulo, una amplia introducción a la ciberseguridad, la ciberdelincuencia, su historia y la estructura que actualmente existe para combatir a los criminales que han hecho del ciberespacio su campo de batalla.

En un momento en el que la conexión entre el rol y el ciberespacio es más estrecha que nunca -sin ir más lejos, casi la totalidad de los materiales de *Karma* solo tienen existencia en este espacio virtual común-, nos ha parecido interesante crear un suplemento que tuviera elementos al respecto para aplicar al juego y, sobre todo, que fuera una puerta para aprender algo más del mundo del ciberespacio, en el que nuestras vidas ya están, de forma irremediable, parcialmente sumergidas. Este suplemento ofrece al lector algunas advertencias útiles que van más allá de la mesa de juego. De hecho, esa es la principal ayuda que encontraréis en estas páginas y la mejor sugerencia que os podemos dar:

Leed al menos los breves consejos básicos que Raquel nos ofrece: pueden ahorraros muchos disgustos más allá de las mesas de juego.

Dimos muchas vueltas a dónde colocar los veinte consejos en los que la autora sintetiza lo que cualquier usuario debe hacer para mantener seguras sus actividades cibernéticas, y optamos por colocarlo al principio, nada más empezar, justo al otro lado de esta presentación. Aunque no te interese nada más de este suplemento, yo de ti, querido lector virtual de *Karma*, daría un cuidadoso paseo por esos veinte consejos.

Si hablamos en términos estrictos de juego, *Caja de herramientas para el especialista en ciberseguridad* os ofrece treinta rasgos vinculados al mundo del ciberespacio para poder incluirlos en vuestros personajes, así como un ramillete de especialidades con las que poder convertir a vuestros personajes en virtuosos del ciberespacio. También encontraréis un amplio listado de posibles actividades, tanto para incursos como para especialistas en ciberseguridad, y una serie de consejos generales sobre cómo introducir cuestiones relativas al ciberespacio en partidas de *Karma*. Por último, tienes un amplio glosario de términos, tanto para guiarte por un campo que puede resultar muy técnico como para que los pongas en boca de tus personajes, utilizando la jerga de los especialistas como una forma más de inmersión en un entorno imaginado.

Hemos cumplido con lo que prometimos. Solo han sido unos instantes. Ya puedes averiguar cómo un ciberataque destrozó los ejes de las centrifugadoras de la central nuclear de Natanz, tratar de desentrañar los códigos de una organización rival, rastrear en la Dark Web los foros de extremistas conspiranoicos o lograr convencer a un alto cargo de un cártel para que te dé las claves de sus cuentas corrientes en Suiza pinchando en el aparentemente inofensivo enlace que has deslizado en la pantalla de su ordenador.

**SI SOLO VAS A LEER UNA COSA DE ESTE
SUPLEMENTO... QUE SEA ESTO**

VEINTE BUENAS PRÁCTICAS PARA EVITAR SER VÍCTIMA DE UN CIBERDELITO

- 1.- Mantén tus equipos, aplicaciones y software actualizados.
- 2.- No abras correos electrónicos provenientes de desconocidos e identifica correctamente al remitente.
- 3.- No proporciones tus datos personales en redes sociales.
- 4.- No instales aplicaciones o software desde plataformas no oficiales. Además, es altamente recomendable utilizar siempre productos de software licenciados, ya sean de código abierto o cerrado.

5.- No aportes ningún tipo de información requerida mediante el correo electrónico, especialmente en lo referente a claves o datos personales.

6.- Evita abrir archivos adjuntos y enlaces a páginas web externas desde el correo electrónico, especialmente si hacen referencia a servicios de banca online, pasarelas de pago o cualquier otro lugar en el que se almacenen datos bancarios, pues podrían ser fraudulentas.

7.- Revisa la existencia de faltas de ortografía, errores de traducción o errores gramaticales en la expresión, pues podrían ser claros indicativos de la recepción de un correo electrónico fraudulento.

8.- Verifica la barra de direcciones del navegador y comprueba si concuerda con la dirección del sitio web oficial.

9.- Asegúrate de que solamente introduces tu información personal y tus claves de acceso en páginas web que utilicen protocolos seguros de comunicación (HTTPS), certificado digital válido e incluyan



el símbolo de un candado (), pues indica que la conexión es segura.

10.- Utiliza el segundo factor de autenticación en aquellas páginas web que lo permitan.

11.- Cambia siempre tus credenciales por defecto (por ejemplo, Router, redes Wi-Fi...) siguiendo el estándar marcado en el paso 12.

12.- Configura credenciales robustas (con ocho o más caracteres, letras mayúsculas y minúsculas, números y caracteres especiales, que no estén asociadas a tus datos personales) y cámbialas cada cierto tiempo, siendo recomendable hacerlo en lapsos de entre uno y tres meses. Si se diese a conocer una filtración de credenciales en un

servicio que utilizases, asegúrate de no utilizar las claves configuradas para ese sitio nunca más.

13.- No reutilices tus credenciales en distintos servicios, siendo recomendable configurar una clave distinta para cada uno de ellos. Para facilitar esta labor, se puede hacer uso de generadores y gestores de contraseñas aleatorias en los cuales se puede especificar la longitud de la contraseña que se desea obtener y el tipo de caracteres que se desea incluir en ella, así como almacenarlas de manera segura.

14.- Elimina los metadatos de tus documentos e imágenes antes de distribuirlos o subirlos a cualquier sitio o página web.

15.- No descargues contenido pirata y revisa siempre la extensión de los ficheros que obtengas, pues podrían contener software malicioso (por ejemplo, si estás descargando un documento con extensión .mp4, sospecha si lo que realmente obtienes es un fichero ejecutable con extensión .exe; ante cualquier indicio de duda, no lo abras).

16.- Realiza una copia de seguridad de toda la información y datos que valores en un sitio externo a tu equipo, para posibilitar que la información pueda ser recuperada en caso de pérdida.

17.- Si te topas con una página web, correo electrónico o contenido susceptible de ser fraudulento, denúncialo a las autoridades o avisa a la entidad afectada, con la finalidad de que se pueda actuar contra los ciberdelincuentes que lo hayan desarrollado.

18.- Evita conectar a tu equipo dispositivos extraíbles desconocidos.

19.- Evita conectar tus dispositivos a redes Wi-Fi públicas o conexiones inalámbricas desconocidas, especialmente en los momentos en los que vayas a interactuar con información sensible. En caso de que

se precise la conexión a este tipo de redes, es altamente recomendable utilizar herramientas de tunelización o servicios VPN.

20.- Desconfía de las llamadas telefónicas provenientes de números desconocidos en las que te soliciten datos personales o bancarios de manera urgente, pues en estas modalidades de estafa online se apremia al individuo a proporcionar sus datos con rapidez, de modo que no llegue a verificar si lo que le indican es cierto. Por norma general, todos los servicios y entidades que actúan de manera legítima, al momento de requerir este tipo de datos al individuo, hacen uso de un sistema telefónico automático que contiene una grabación en la que solicita la información necesaria, con la finalidad de que ninguna persona llegue a conocer la información requerida.

No queremos dejar de agradecer a Raquel Puebla las muchas horas de su escaso tiempo invertidos en elaborar, de forma completamente desinteresada, tanto estos consejos como el resto de material informativo que contiene la primera parte de este suplemento.

Sin personas como ella, este y otros proyectos de todo tipo no podrían seguir adelante y en el océano confuso en que vivimos faltaría, al menos, esa gota radiante.

PARTE I:

**PANORAMA DE CIBERSEGURIDAD
ACTUAL**

**-Raquel Puebla González-
Entelgy Innotec Security**

CAPÍTULO I: CONCEPTOS BÁSICOS DE CIBERSEGURIDAD

1.-Origen de la ciberseguridad

La ciberseguridad, también denominada seguridad informática o seguridad de tecnologías de la información, es la disciplina encargada específicamente de la protección de la información contenida o transferida a través de la tecnología informática. En un sentido más amplio, también es el área que se encarga de la protección de la infraestructura computacional y todo aquello relacionado con la computación.

Si bien es una disciplina reciente, que solo cuenta con unas pocas décadas de desarrollo, la seguridad informática ha experimentado grandes cambios desde sus orígenes a la actualidad.

Entre los años 1980 y principios de 1990, la ciberseguridad estaba enfocada principalmente a asegurar el funcionamiento de los dispositivos informáticos, concretamente los ordenadores. Por ende, la protección se centraba en actuar contra infecciones provocadas por determinados virus informáticos.

Sin embargo, la ciberseguridad, tal y como la entendemos hoy, nace como consecuencia del desarrollo masivo de Internet y la conectividad de las redes. Surge también como respuesta a la creciente necesidad de proteger la información, que se encuentra al alcance de un mayor número de individuos y expuesta a multitud de riesgos.

Debido a lo anterior, la ciberseguridad está estrechamente relacionada con la seguridad de la información, disciplina que se encarga de salvaguardar tres principios básicos:

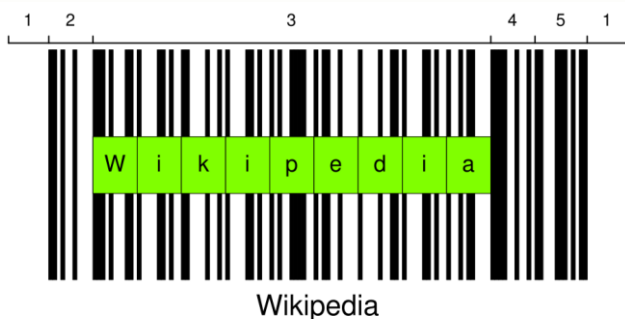
- La confidencialidad, que tiene como finalidad impedir el acceso no autorizado a la información.
- La integridad de los datos, que sirve al propósito de conservar la información sin alteraciones ni modificaciones que no hayan sido autorizadas previamente.
- La disponibilidad, que tiene como objetivo que la información pueda ser utilizada en todo momento, sin interrupciones.

En adición a estos tres principios básicos, con el tiempo se han ido contemplando otras dimensiones o propiedades que los complementan y contribuyen a preservar la seguridad de la información:

- La autenticidad es la característica que permite identificar la fuente de la que emana la información, aquella propiedad que permite determinar su procedencia, quién es su autor o la entidad que la emite.
- El no repudio, también conocido como irrenunciabilidad, es la característica que permite aseverar la intervención del emisor y el receptor en la comunicación. Por tanto, es la

propiedad que impide que el emisor pueda negar el envío de la comunicación (no repudio en origen) y que el emisor pueda negar la recepción del mensaje (no repudio en destino) porque la otra parte de la comunicación puede aportar pruebas del envío o de la recepción del mensaje, según el caso.

- La trazabilidad, también conocida como auditabilidad, es la característica que permite atribuir cualquier actividad o actuación, como modificaciones o accesos a cierta información, a un determinado usuario o entidad, de manera que se requiere la realización de labores de monitorización y registro que permitan efectuar una identificación correcta de los actores que hayan participado en la comunicación.



- Los códigos de barras son un ejemplo de trazabilidad; en la imagen, un ejemplo de Wikipedia-

Como consecuencia de su propio desarrollo, las implicaciones de la seguridad informática también han crecido exponencialmente, pues la perpetración de un ataque ya no tiene la finalidad exclusiva de corromper un sistema, sino que afecta a derechos fundamentales de los individuos.

2.- Amenazas principales a la seguridad informática

Como consecuencia del desarrollo de las tecnologías de la información y la comunicación, así como con la aparición del escenario de la ciberseguridad, han surgido nuevas amenazas que podrían llegar a producir algún tipo de impacto tanto sobre los sistemas de los usuarios a nivel individual como a nivel colectivo en el ámbito corporativo, pudiendo afectar a entidades gubernamentales y a distintas organizaciones tanto del sector público como del sector privado.

En relación con lo anterior, actualmente existen tres amenazas principales que desafían al panorama de la ciberseguridad actual: el cibercrimen, la ciberguerra y el ciberterrorismo. La diferencia principal entre estos tipos de amenazas radica en su motivación:

- El objetivo primordial del cibercrimen es la consecución de un lucro económico.
- El propósito de la ciberguerra es la consecución de determinados objetivos políticos.
- La finalidad del ciberterrorismo consiste en provocar e infundir miedo e inestabilidad.

La cibercriminalidad, también conocida como ciberdelincuencia, fue abordada por primera vez en el contexto internacional con el Convenio sobre Cibercriminalidad o Convenio de Budapest, que entró en vigor el 1 de julio de 2004, si bien no fue ratificado por España hasta el 1 de octubre de 2010. En él se definen como ilícitos penales determinadas conductas entre las que se incluyen diversas actividades que atentan directamente contra la confidencialidad, integridad y/o disponibilidad de los datos y de los sistemas informáticos o contra la propiedad intelectual, la falsificación, el fraude y actividades relacionadas con la pornografía infantil.

Por otro lado, cabe decir que, en ocasiones, el concepto de ciberguerra se equipara o confunde con el de ciberactivismo. Ambos conceptos persiguen la misma finalidad: la consecución de determinados ideales o fines políticos. En la ciberguerra los atacantes, principalmente pertenecientes a una organización nacional o supranacional, realizan labores de ciberespionaje y robos de información muy sensible que pueden desgastar o debilitar a una nación objetivo. En un caso de ciberguerra más abierto, los ataques podrían ser dirigidos contra infraestructuras críticas, las cuales, una vez deterioradas, podrían causar tanto daño como una bomba en el escenario tradicional de guerra. Es por ello que los cibercombatientes también requieren de una instrucción técnica previa y de la elaboración de una estrategia que les permita llevar a cabo estos ataques. Aún con todo, no se ha llegado a un consenso que explique de forma exacta el concepto de ciberguerra y algunos profesionales siguen dudando acerca de si existe en realidad.



Centro de ciberseguridad de la US Navy

Por otro lado, el ciberactivismo es un movimiento social y político en la red del que prácticamente cualquier usuario puede ser partícipe, pues persigue la denuncia y la protesta sobre una temática, como la política, la defensa del medio ambiente o los abusos de los derechos humanos, valiéndose para ello de la viralización de determinados contenidos y cualquier otra acción política en la red.

El ciberactivismo es, por tanto, una forma pacífica de protesta en la que se utilizan los medios digitales para propagar un mensaje específico en torno a un problema social o político. Sin embargo, existe una vertiente del ciberactivismo, conocida como hacktivismo, en la que se emprenden acciones ilegales en la red para alcanzar los mismos objetivos que en el ciberactivismo pacífico. El término proviene de la unión de los términos “*hacking*” y “activismo”. Del primero se desprende la necesidad de que la persona hacktivista posea los conocimientos técnicos necesarios para llevar a cabo ciberataques que generalmente no revisten especial importancia y no producen grandes consecuencias; mientras que el segundo término hace referencia a la consecución de los objetivos sociales y políticos de los que se hablaba con anterioridad. No obstante, cabe señalar que los actores que operan dentro del hacktivismo, al llevar a cabo actividades, protestas y reivindicaciones de muy diversa índole, en muchas ocasiones pueden acometer acciones que puedan ser susceptibles de ser englobadas dentro de la cibercriminalidad, el ciberterrorismo o incluso la ciberguerra, en función de la finalidad y los objetivos que persigan en cada momento.

Por último, el ciberterrorismo nace de la unión de la ciberdelincuencia y el terrorismo, de modo que consiste en un tipo de delito cibernético al igual que los señalados en el párrafo relacionado con la cibercriminalidad, con la salvedad de que, en este caso, los ciberataques no se perpetran con el propósito de conseguir lucro económico, sino que se llevan a cabo con la finalidad de intimidar a un gobierno o a su población para alcanzar determinados fines políticos o sociales.

En relación con los términos anteriores y con el panorama de la ciberseguridad, es preciso hacer mención a otro concepto, el de ciberespacio. El ciberespacio es el entorno que hace posible la existencia de todas estas nuevas acepciones. Una nueva dimensión fruto del surgimiento de las TIC (Tecnologías de la información y el conocimiento), que ha permitido el traslado de actividades habitualmente vinculadas al espacio físico, como la enseñanza, el trabajo, las relaciones entre individuos de cualquier índole o la compraventa, entre muchos otros, a un entorno virtual, intangible e ilimitado, capaz de cambiar los hábitos, la sociedad en su conjunto y la forma de relacionarse con ella.



El ciberespacio es un concepto difuso y abstracto, es un espacio virtual donde, a partir de ciertos tipos de software, redes, tecnologías, dispositivos, etcétera, se pueden crear y diseñar elementos que no

existen en forma física pero sí de manera lógica, con los que se puede interactuar al igual que podría hacerse en el espacio real. En este sentido, Internet, como la mayor red de redes que existe actualmente, ha constituido la plataforma mayoritaria que posibilita que se pueda operar dentro del ciberespacio, aportando la infraestructura (máquinas, software, tecnologías, protocolos, etcétera) necesaria para proporcionar soporte a las comunicaciones entre distintos sistemas. Por tanto, aunque ambos términos se confunden en ocasiones, se puede determinar una jerarquía entre ambos conceptos, pues si el ciberespacio constituye una dimensión, al igual que la tierra, el aire, el mar y el espacio exterior, donde se puede interactuar y donde tienen lugar acontecimientos, Internet es el mecanismo que, mediante el conjunto de redes que lo conforman, permite que este nuevo tipo de interacción sea posible, de forma que, aunque pueda existir cierta dependencia entre ambos conceptos, se puede afirmar que Internet forma parte del ciberespacio, que este lo engloba y que, además, conforma un concepto más amplio y complejo que lo que se conoce como Internet. En este sentido, cabe señalar otra serie de conexiones no dependientes de Internet que también forman parte del ciberespacio, como las conexiones bluetooth, por satélite, las conexiones cifradas como Freenet, VPN, i2p y Tor, además de las redes de telefonía, que utilizan conexión GSM. Todas ellas forman parte del ciberespacio y permiten crear una conexión entre dos o más dispositivos sin necesidad de que intervenga Internet.

En relación con cualquiera de las amenazas expresadas con anterioridad, los atacantes utilizan una serie de técnicas, herramientas y vectores de ataque para llevar a cabo sus acciones delictivas y que éstas obtengan el éxito esperado, entre las cuales se encuentran algunas como el malware, la explotación de vulnerabilidades y la ingeniería social.

Malware es la denominación estándar que se otorga a cualquier tipo de software cuya finalidad es comprometer un dispositivo o infiltrarse en él sin contar con la autorización y el conocimiento de su propietario. Este término, procedente del inglés, es fruto de la unión de las palabras “*malicious software*”, que en castellano significa código

daño o software malicioso. Cabe señalar que, en sus comienzos, el malware lo constituían piezas de software que realizaban algún tipo de actividad maliciosa. Por esta razón se hablaba, e incluso actualmente se hace referencia a ello, de tipologías de malware cuando, en el fondo, se deberían referenciar sus características, puesto que el malware moderno no sólo efectúa una función, sino que puede llevar a cabo acciones diferentes y siendo, a su vez, modular. Así pues, se exponen a continuación características comunes en el malware que, como se ha indicado, en ocasiones definirán bien una familia, bien una funcionalidad, bien una manera de replicarse. Hay que advertir también que muchos de los nombres tuvieron un significado cuando se les puso y que, con el tiempo, este ha ido variando:

- **Virus:** característica del malware que indica que, independientemente de su objetivo, el código busca replicarse modificando otros ficheros del sistema, pasando desapercibido e infectando otros sistemas al copiar esos archivos. Aunque esa es la terminología que mejor caracteriza el concepto de “virus”, el término es empleado para referirse al malware en general, a consecuencia de que los medios de comunicación extendieron la utilización del término como símil con los virus que afectan a los seres humanos.

- **Gusano o *Worm*:** característica del malware que indica que el código se replica a través de la red en distintos ordenadores haciendo uso de vulnerabilidades en otros sistemas, credenciales robadas o débiles, o dispositivos extraíbles.

```

0 00 00-6D 73 62 6C          mshl
0 6A 75-73 74 20 77          ast.exe I just w
9 20 4C-4F 56 45 20          ant to say LOVE
0 62 69-6C 6C 79 20          YOU SAN!! billy
0 64 6F-20 79 6F 75          gates why do you
3 20 70-6F 73 73 69          make this possi
0 20 6D-61 6B 69 6E          ble ? Stop makin
E 64 20-66 69 78 20          g money and fix
7 61 72-65 21 21 00          your software!!
0 00 00-7F 00 00 00          ♣ ♂♥▶ H △
0 00 00-01 00 01 00          ♂_♂_ ⊙ ⊙ ⊙
0 00 00-00 00 00 46          á⊙ L ⊙ F
C C9 11-9F E8 08 00          ♠ jêèù-⌂⌂f⌂⌂
0 00 03-10 00 00 00          +▶H'⊙ ♣♥▶
3 00 00-01 00 04 00          ♠♥ ò ♂♥ ⊙ ♠

```

-Código del gusano Blaster, que incluye un mensaje para Bill Gates-

- *Spyware* o *Stealer*: característica del malware que indica que el código tiene la intencionalidad de espiar las acciones del usuario, pudiendo robar sus datos de navegación, tomar pantallazos del escritorio o robar ficheros del sistema, entre otros. Dentro del spyware o stealer existen varias sub-características que conviene señalar:

- *Keylogger*: sub-característica del *spyware* en la que el *malware* roba las pulsaciones de teclado, registrando toda la información que introduce el usuario mediante ese modo, quedándose igualmente con usuarios, contraseñas e información muy variada.

- *Form grabber*: sub-característica del *spyware* en la que el *malware* roba la información que los navegadores remiten al servidor web cuando el usuario completa cualquier formulario y lo envía mediante la pulsación del botón correspondiente, generalmente “enviar” o “ir”. Habitualmente el código es

incorporado en el navegador del usuario cuando éste instala alguna extensión o barra de herramientas que haya sido especialmente diseñada para contribuir a esta finalidad, mientras que, en otros casos, el software intercepta alguna llamada dentro del sistema relacionada con el envío de información mediante el protocolo HTTP. Los *form grabbers* nacen como consecuencia de las limitaciones existentes en los *keyloggers*, que impiden la obtención de información cuando el usuario utiliza la técnica de copiar y pegar en lugar de introducir la información mediante el teclado, al igual que ocurre con las listas desplegables, en las que el usuario elige con el ratón una opción de entre varias que se le ofrecen.

○ *Banker*: sub-característica del *spyware* en la que el *malware* roba las credenciales bancarias de los usuarios afectados, con la finalidad de hacerse con el control de sus cuentas, recopilando información acerca de sus conexiones bancarias y, en muchos casos, modificando su navegación con la finalidad de engañarles para cometer distintos tipos de ciberdelitos. Ese tipo de *malware* se diseña especialmente para recopilar distintos datos bancarios del usuario, como sus credenciales para banca online o la numeración de sus tarjetas de crédito y débito, entre otros.

- *Adware*: característica del *malware* que indica que el código añade publicidad en el ordenador infectado, comúnmente en su navegación por Internet, agregando *popups*, clicks maliciosos, cambiando el resultado cuando se hace uso de buscadores, etcétera. Con cierta frecuencia, este tipo de *malware* se incluye en la instalación por defecto del dispositivo aparentando ser algún tipo de software gratuito (*freeware*) o con licencia restringida (*shareware*), motivo por el cual el usuario debe modificar los parámetros mediante una instalación avanzada.

- *Downloader* o *Loader*: característica del malware que indica que el código descarga aplicaciones que instala o ejecuta en el equipo de la víctima sin que ella se dé cuenta, pudiendo así añadir otras funcionalidades maliciosas. Esta es una de las maneras de hacer el malware modular.

- *Scareware*: característica del malware que indica que el código tiene la intencionalidad de asustar a la víctima, por ejemplo, con la finalidad de pedir dinero por unas fotos comprometidas (que no existen realmente) o por una falsa acusación de tener pornografía infantil en el ordenador. En ocasiones, este software malicioso es utilizado para advertir a las víctimas de que su equipo ha sido infectado con un virus que en realidad es falso y le invitan a adquirir un antivirus que supuestamente elimina la amenaza identificada y que tampoco es real.

- *FakeAV*: característica del malware que indica que el código se hace pasar por un antivirus para que el usuario se lo instale pensando que está protegido cuando, lo que realmente hace, es alguna otra funcionalidad maliciosa.

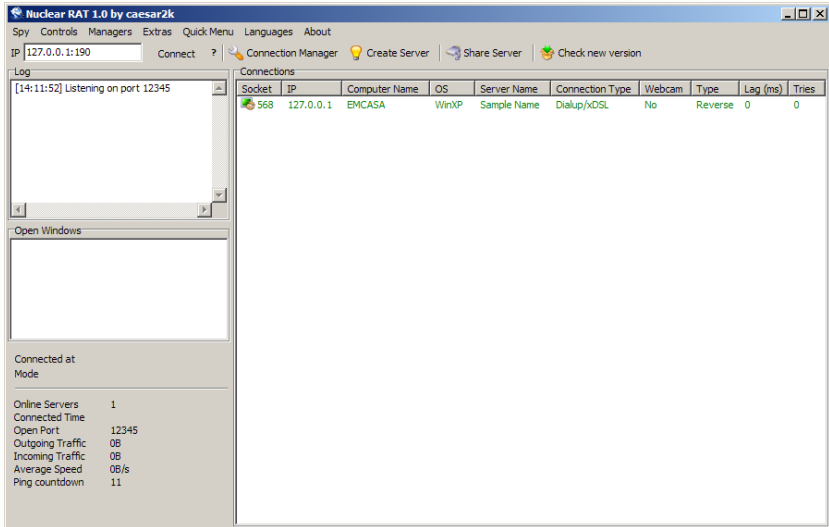
- *Backdoor*: característica del malware que indica que el código establece un acceso remoto en el equipo infectado permitiendo, normalmente, su control en remoto.

- *Rootkit*: técnica que permite al malware ocultarse en el sistema modificando ciertos archivos o ciertas llamadas al propio kernel o núcleo del sistema, de forma que se evita mostrar su presencia, lo que hace muy complicado su detección.

- *Ransomware*: característica del malware que indica que el código cifra parte del sistema, normalmente los datos de los usuarios, o bien todo el sistema, bloqueando el acceso a los usuarios a la información y/o servicios que éste ofrece, pidiendo un rescate a cambio

de su recuperación, normalmente en alguna criptomoneda como Bitcoin.

- **Mineros:** característica del malware que indica que el código se instala en el ordenador para llevar a cabo un proceso de minado mediante el cual se consume la capacidad de procesamiento del sistema infectado con la finalidad de producir criptomonedas.



- Imagen del troyano Nuclear Rat.-


- **Troyano o Trojan:** es la característica del malware cuyo concepto más ha variado a lo largo del tiempo. Inicialmente, hacía referencia al software que simulaba constituir un programa legítimo o útil con la finalidad de que el usuario lo instalase y ejecutase, mientras que en su interior contenía la carga maliciosa. El software era a veces el real, pero con la carga maliciosa dentro, y a veces un software falso, igualmente con la carga maliciosa dentro, como los falsos antivirus

(FakeAV). Con el tiempo, ese nombre se empezó a utilizar como un término genérico para describir cualquier malware que se instalaba en el ordenador y proporcionaba al atacante control externo (Backdoor). A día de hoy, se usa para definir cualquier malware que se instala en el ordenador. Además, tomando en consideración que la práctica totalidad de los troyanos poseen una funcionalidad de control remoto, lo que se conoce en inglés como *Remote Access Tool* (RAT), en la actualidad también se relacionan los troyanos con cualquier pieza de malware que contenga esta característica.

Vulnerabilidad es la denominación que se otorga a todas aquellas debilidades o fallos que se producen en los sistemas informáticos. Las vulnerabilidades constituyen un riesgo grave que, de ser aprovechado por los atacantes, atenta directamente contra los principios básicos de la seguridad de la información. En relación con este término, un exploit se define como el programa o fragmento de código cuya finalidad es aprovechar o explotar dicha vulnerabilidad. Expresado de otro modo, los atacantes tratan de aprovechar una determinada vulnerabilidad, o varias, mediante el desarrollo de un nuevo exploit o la utilización de otro ya existente para obtener una vía de acceso al sistema, la cual podría ser utilizada posteriormente para realizar otro tipo de actividades maliciosas, como el despliegue de un determinado malware.

Ingeniería social es la denominación que se otorga a todas las técnicas que, a diferencia de las herramientas y vectores de ataques anteriores, se sustentan sobre la manipulación psicológica y el engaño de la víctima, motivo por el cual existe un componente de interacción humana. De tener éxito, los atacantes consiguen su objetivo, sea cual sea, debido a las acciones que emprende la víctima sobre su propio equipo, sin necesidad de que sean ellos los que deban comprometerlo directamente. Una de las técnicas de ingeniería social más comunes es el phishing, un tipo de estafa cibernética que consiste en la emisión de una comunicación electrónica aparentemente oficial a la víctima, por lo general mediante correo electrónico, en la que el atacante finge ser una

entidad legítima o de confianza que solicita al usuario realizar alguna acción, generalmente facilitar determinados datos.



PROTECT YOUR INFO!
PSEC ALERT

What is social engineering?

Social engineering is the art of manipulating people into performing actions or divulging confidential information, rather than by breaking in or using technical cracking techniques. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud or computer system access; in most cases the attacker never comes face-to-face with the victim. Social engineering using impersonation (e.g. to gain information over the phone, or to gate-crash) is known informally as blagging. In addition to criminal purposes, social engineering has also been employed by debt collectors, skip tracers, private investigators, bounty hunters and tabloid journalists. A study by Google researchers found that up to 90 percent of all domains involved in distributing fake antivirus software used social engineering techniques.

También existen otros tipos de ataques bastante comunes que persiguen disminuir la capacidad que tiene un servicio o una red para prestar un servicio con cierto grado de calidad. Estos ataques son conocidos como denegaciones de servicio. Para ejecutar esta clase de ciberataques, los actores que los llevan a cabo envían un número elevado de peticiones al servidor hasta que este colapsa ante la imposibilidad de que todas ellas puedan ser atendidas. En caso de tener éxito, las denegaciones de servicio provocan la interrupción total o parcial del servicio, de modo que se vuelve inaccesible para todo aquel que intente acceder al recurso mientras dure el ataque. Para provocar el colapso del servidor, los atacantes pueden enviar las peticiones desde una única dirección IP u ordenador, lo que se conoce como denegación de servicio (DoS), o desde distintas direcciones IP o equipos, lo que se conoce como denegación de servicio distribuida (DDoS). En ocasiones, las denegaciones de servicio se producen de forma no intencionada al colapsar el servidor o la red al lanzar un gran número de peticiones.



-Web bloqueada por el FBI con relación a un ataque DDoS-

También en relación con tipos comunes de ciberataques se encuentra lo que se conoce como ataques de intermediario, más conocidos como Man in the Middle (MitM). La técnica Man in the Middle consiste en una irrupción dentro del canal de comunicación entre el cliente y el servidor con la finalidad de interceptar el tráfico que se realiza entre ambos. El objetivo de la técnica es modificar o simplemente observar el flujo de información que transcurre, pudiendo, por tanto, provocar filtraciones y robos de información susceptible de ser restringida, sensible o confidencial. Durante la realización de este tipo de ataques, el actor constituye una pasarela entre el cliente y el servidor para obtener la información que circula entre ellos y después la envía al servidor para evitar ser detectado y aparentar normalidad en la red.

De forma general, los ciberdelincuentes llevan a cabo ciberataques en los que se dirigen a un gran número de víctimas en el menor tiempo posible. Estos ataques son indiscriminados y no suelen contar con demasiada complejidad ni preparación. Por ese motivo en los ataques tradicionales se suelen emplear técnicas como las anteriores, infecciones por malware o la ingeniería social. En muchos casos estos ataques se solucionan con la instalación o actualización de un antivirus.

No obstante, también existen otros tipos de ataques mucho más sofisticados que requieren de mayor desarrollo y planificación, motivo por el cual suelen ser llevados a cabo por actores con recursos que pertenecen a organizaciones criminales. En un ataque dirigido los actores definen previamente sus objetivos, métodos y alcance, con lo cual la investigación que precede al ataque, así como su grado de planificación y complejidad son muy altos. Las víctimas de un ataque de este tipo se escogen meticulosamente y nunca son masivas, indiscriminadas o aleatorias, sino que el ataque se destina a un público objetivo concreto.

Existen dos tipos de técnicas que se utilizan en los ataques dirigidos: las Amenazas Volátiles Avanzadas, cuyo acrónimo, derivado del nombre que recibe en inglés - *Advanced Volatile Threat* -, es AVT; y las Amenazas Persistentes Avanzadas, cuyo acrónimo, derivado del nombre que recibe en inglés - *Advanced Persistent Threat* -, es APT.

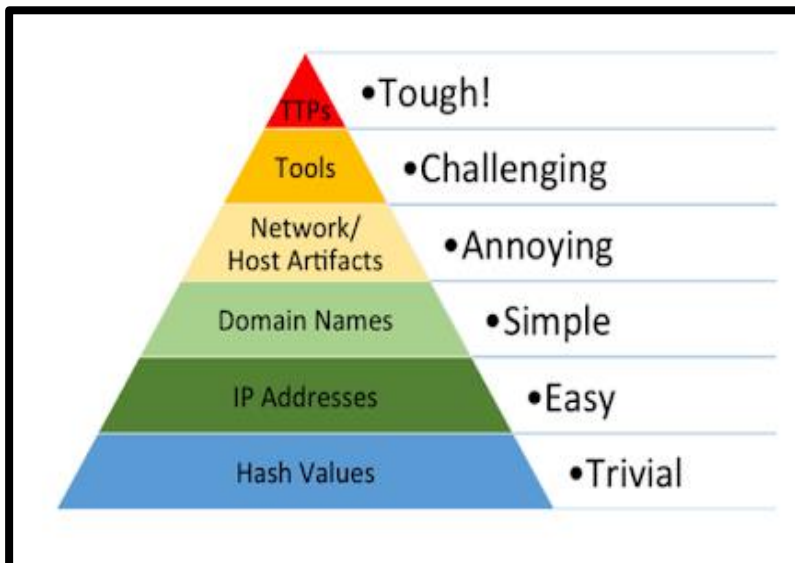
Las Amenazas Volátiles Avanzadas (AVT) son ataques que se guardan en la memoria RAM de los dispositivos del objetivo al que se dirigen, de modo que desaparecen en el momento en el que esos dispositivos se reinician. Debido a su utilidad, estas técnicas son empleadas generalmente en labores de espionaje, puesto que cuando consiguen robar la propiedad intelectual de su objetivo desaparecen muy rápidamente y no dejan rastro que las identifique.

Por el contrario, las Amenazas Persistentes Avanzadas (APT) son ataques que se guardan en el disco duro de los dispositivos del objetivo al que se dirigen, de modo que son persistentes al reinicio del dispositivo. Es decir, no desaparecen, sino que pueden perdurar durante meses e incluso años dentro del sistema. Para poder llevar a cabo estas técnicas se requiere que los atacantes posean grandes conocimientos técnicos, tanto en programación como en seguridad de la información, y recursos que permitan combinar diferentes herramientas como aquellas de las que se hablaba con anterioridad.

Cuando se realiza un ataque dirigido basado en una Amenaza Persistente Avanzada, este se dirige a los recursos de red de un determinado objetivo que posee información de valor para los actores que lo han llevado a cabo. Para conseguirlo, en la fase previa de planificación escogen un objetivo más sencillo que, a pesar de no aportar información de valor, se encuentra en la misma red que el objetivo real. Si el atacante consigue comprometer ese sistema y escalar privilegios hasta acceder a su verdadero objetivo podrá conseguir el acceso a la información que desea. Las herramientas que se utilizan en este tipo de ataques están especialmente diseñadas para sobrepasar y adaptarse a las medidas de defensa y seguridad del objetivo escogido, de modo que la APT puede mantenerse activa en la red de la víctima durante años. Por tanto, la persistencia de la amenaza permite extraer datos y ejercer un monitoreo de forma continuada durante largos periodos de tiempo.

Por otro lado, cabe decir que, en ocasiones, debido a la ausencia de consenso entre los profesionales del sector, el acrónimo APT se utiliza erróneamente para referirse a aquellos grupos de actores que inician campañas en las que se perpetran ataques basados en técnicas del tipo APT.

Existen diferentes escalones de dificultad a la hora de investigar un ataque, igual que ocurre al momento de perpetrarlos. Esto se ilustra, generalmente, con una pirámide orientada a la ciberseguridad comúnmente denominada Pirámide TTP (Técnicas, Tácticas y Procedimientos) o Pirámide del Dolor.



Fuente: León, D. (2018). TTPs y la Pirámide del Dolor. Zerolynx. Recuperado de <https://blog.zerolynx.com/2018/04/ttps-y-la-piramide-del-dolor.html>.

En el escalón más bajo de la pirámide se encuentran los hashes. Un hash es un algoritmo matemático que permite identificar un fichero o cualquier activo digital de forma inequívoca. Esto se debe a que cada hash es único, de modo que, si se modifica cualquier parte del fichero, se genera otro hash que lo identifica. Existen diferentes tipos de hashes según la manera en la que se calcule su algoritmo, siendo los más

comunes los denominados md5, sha1, sha256 y ssdeep. Como cada hash es único, resulta muy sencillo para los investigadores comprobar, mediante su análisis, si un fichero es legítimo o si se encuentra modificado por algún tipo de malware, puesto que, en este último caso, el hash sería distinto al del fichero original. Por tal motivo, en la pirámide reciben la calificación de “Trivial” (nivel muy bajo). Como contrapartida, también son muy fáciles de variar por los atacantes, puesto que en el momento en el que éstos modifiquen cualquier fragmento del malware, su hash también habrá variado. Por tanto, cuando los investigadores de seguridad se sitúan en este escalón de la pirámide se considera que poseen un nivel de conocimiento muy bajo sobre los actores que investigan.

En el siguiente peldaño de la pirámide se encuentran las direcciones IP que, al igual que ocurre con los hashes, son relativamente fáciles de cambiar. Una dirección IP, cuyo acrónimo procede del inglés – *Internet Protocol* -, es un número que se asigna a cada usuario o que éste elige al conectarse a la red, mediante el cual se le identifica. Como consecuencia de la gran cantidad de información que aportan (geolocalización, propietario, etcétera) su investigación resulta sencilla para los Equipos de Detección y Respuesta a Incidentes de Seguridad, motivo por el cual se clasifica como “Fácil” (nivel bajo). Sin embargo, no proporcionan demasiada utilidad a los investigadores porque también son rápidas y fáciles de cambiar por otras. Estos cambios entre direcciones IP se pueden realizar de diferentes maneras, bien mediante el uso de alguna VPN (*Virtual Private Network*), desde algún Proxy, o bien desde alguna página web especialmente diseñada para ello.

En el escalón inmediatamente superior al de las direcciones IP se encuentran los nombres de dominio. Un dominio es el nombre mediante el cual se identifica de manera exclusiva a toda página o sitio web. Dicho de otra forma, es la traducción de cada dirección IP a un nombre legible y memorizable para cualquier usuario. Los nombres de dominio también son relativamente fáciles de rastrear y aportan bastante información, motivo por el cual reciben la clasificación de “Sencillo”

(nivel medio-bajo) en la pirámide. Sin embargo, requieren algo más de investigación que las direcciones IP porque se pueden mover de forma geográfica en Internet, recibiendo diferentes direcciones IP cada vez. Además, existen empresas registradoras de nombres de dominio que garantizan el anonimato del registrante. Al igual que ocurre con las direcciones IP, modificar un dominio por otro o utilizar subdominios gratuitos es algo muy sencillo de realizar por casi cualquier actor. Por ende, si bien a un investigador le resulta relativamente fácil conocerlo, tampoco le aporta demasiada utilidad a la hora de investigar un ataque.

Estos tres primeros peldaños de la pirámide contienen indicadores de compromiso que, como se ha afirmado anteriormente, resultan sencillos de conocer y analizar. Los indicadores de compromiso son muestras que evidencian que un equipo ha sido comprometido mediante un ataque. Por tanto, estos indicadores se almacenan y actualizan fluida y constantemente en diferentes bases de datos con las que cuentan los investigadores para que las amenazas de ataques sean detectadas y neutralizadas rápidamente. Esta forma de reaccionar ante las amenazas se denomina Inteligencia Operacional, puesto que, mediante la introducción de los indicadores anteriores en las bases de datos y su mantenimiento, las amenazas se deberían poder detectar de forma automática.

En el siguiente nivel de la pirámide se encuentran los equipos y artefactos de red, que reciben la calificación de “Molesto” (nivel medio-alto) si se traduce el término de forma literal. En el momento en el que los actores se introducen en un equipo o un artefacto conectados a través de la red, les resulta mucho más difícil no dejar huella que evidencie su actividad. Estas evidencias pueden estar constituidas por los logs, que permiten a los investigadores conocer las conexiones y las peticiones que han realizado los actores a un determinado sitio, las claves de registro, patrones de URI que se repiten, algoritmos de exclusión mutua, la versión del sistema operativo y resto de datos del equipo utilizado, etcétera. Como todos estos datos son mucho más difíciles de modificar que cualquiera de los que se encuentran en los escalones anteriores de

la pirámide y, además, son más difíciles de ocultar, poseer información al respecto reviste mayor importancia para los investigadores, puesto que pueden comenzar a establecer ciertos patrones de conducta.

En el peldaño inmediatamente superior de la pirámide se encuentran las herramientas (familias de malware, exploits, etcétera), que se han clasificado con un nivel de dificultad “Desafiante” (nivel alto), si se traduce el término de forma literal, debido a que resulta mucho más complicado para los atacantes desarrollarlas y para los investigadores conocerlas. No obstante, una vez son conocidas por los Equipos de Detección y Respuesta a Incidentes de Seguridad, éstos pueden desarrollar y generar reglas que permiten su detección de forma automática, motivo por el cual su nivel de conocimiento acerca de los actores es mucho mayor. Como consecuencia de la existencia de estas reglas de detección, que pueden ser del tipo YARA o SNORT entre otras, los actores se ven obligados a modificar las herramientas que utilizan y a generar otras nuevas que sean, al menos al principio, indetectables mediante estos métodos. Por ende, investigadores y atacantes se encuentran siempre en constante desarrollo y análisis de nuevas formas de penetrar en los sistemas.

Finalmente, en el último escalón de la pirámide se encuentran las denominadas Tácticas, Técnicas y Procedimientos (TTP’s), a las que se ha atribuido un nivel de dificultad “Difícil” (muy alto). Esto se debe a que exige una investigación muy profunda sobre los actores, de modo que los analistas lleguen a conocer de forma global su comportamiento, su forma de actuar, sus hábitos, los objetivos a los que normalmente atacan, el ámbito geográfico en el que operan, su finalidad, etcétera. Por tanto, el conocimiento que poseen los investigadores que se encuentran en la cúspide de la pirámide acerca de los actores a los que investigan es suficiente como para prevenir y anticiparse a acciones futuras y para neutralizarlas con las mínimas consecuencias cuando no haya sido posible anticiparse a ellas. Además, en este punto a los actores les resulta muy complejo adaptarse a la capacidad que tienen los Equipos de Detección y Respuesta a Incidentes de Seguridad para neutralizar sus

actividades, debiendo asumir grandes costes económicos que les permitan reestructurarse y desarrollarse a nivel interno para cambiar la forma que tienen de operar. Esto, además, no lo pueden realizar de forma sencilla o rápida como ocurriría con la modificación de un hash, sino que se extiende mucho más en el tiempo.

Desde un punto de vista más sencillo, se puede observar la pirámide de forma ascendente, de modo que, cuantos más escalones hayan alcanzado los investigadores de seguridad, más alto será el nivel de defensa y protección con el que cuente la organización y, por tanto, será más difícil que un actor pueda perpetrar un ataque exitoso que comprometa sus sistemas.

Estos tres últimos peldaños de la pirámide contienen indicadores de compromiso que, en muchos casos, hacen referencia a los patrones de conducta y al *modus operandi* de los actores, los cuales no se pueden conocer sin llevar a cabo una investigación profunda y continuada en el tiempo. Este nivel de análisis se engloba dentro de la denominada Inteligencia Táctica y Estratégica, que, como su propio nombre indica, tiene como objetivo la consecución de un conocimiento profundo sobre los actores para poder elaborar estrategias que disminuyan su capacidad operativa.

En ocasiones, el escalón de la pirámide conformado por las Tácticas, Técnicas y Procedimientos se supedita a otro nivel adicional en el que se engloba la Contrainteligencia. Ésta es entendida como aquellas técnicas con las que se engaña a los actores mediante la utilización de señuelos para que éstos crean que están perpetrando un ataque exitoso cuando en realidad están contribuyendo a su propia investigación. A través de estas técnicas los analistas pueden extraer información valiosa que les permita reforzar sus sistemas de defensa y crear medidas de defensa adicionales.

Para concluir este apartado introductorio sobre las amenazas principales a la seguridad informática es necesario diferenciar algunos conceptos que hacen referencia a los niveles o partes de Internet en los que pueden operar los actores anteriores. Algunos de estos términos, muy populares últimamente en los medios de comunicación, pero no muy bien distinguidos generalmente, son Clearnet, Deep Web, Dark Web y Darknet.

La Clearnet o Red de Superficie es aquella parte de Internet fácilmente accesible para cualquier usuario desde cualquier navegador, de modo que puede introducirse sin dificultad en páginas web indexadas por motores de búsqueda convencionales como Google, Yahoo o Bing y en otra serie de sitios web a los que, a pesar de no encontrarse indexados en los buscadores anteriores, se puede acceder de forma pública, tal y como ocurre con los blogs o con redes sociales como Facebook y Twitter. La Clearnet, además, permite generalmente la geolocalización del usuario mediante la búsqueda de su dirección IP de un modo sencillo. Si bien es la parte de Internet más popularizada y recurrida entre los usuarios, llegándose a estimar que alrededor del 90% accede casi exclusivamente a la Clearnet, cabe decir que representa un porcentaje muy pequeño de la totalidad de Internet, abarcando alrededor de entre un 4% y un 10%.

La Deep Web o Internet Profunda, por el contrario, es la capa profunda de Internet. Abarca alrededor del 90% de su totalidad e incluye todas las páginas y sitios web que no pueden ser indexados por los buscadores tradicionales. Además, también representa aquellas páginas web que no están abiertas al público en general, sino que requieren de un registro previo, así como los servicios de correo electrónico, en los cuales cada usuario solamente puede acceder al suyo propio, y las bases de datos.

La Dark Web o Internet Oscura y la Darknet son dos conceptos muy relacionados entre sí. El primero de ellos, la Dark Web, constituye una pequeña porción (alrededor del 0,1%) de la Deep Web. Está

formada por todo el contenido que ha sido ocultado de forma deliberada y que solamente es accesible a través de las Darknets, esto es, redes a las que el usuario solo se puede introducir mediante herramientas y programas específicos con los que se persigue su anonimato, pues permiten ocultar su identidad, geolocalización y actividad. Los programas más conocidos para obtener acceso y navegar por la Dark Web son TOR, I2P y Freenet. A esta característica de la Dark Web, que proporciona anonimato al usuario, se debe que se haya popularizado su uso entre diferentes grupos de ciberdelincuentes, de modo que, entre otros contenidos que pueden ser legales o no, es posible encontrar en ella fácilmente servicios de tráfico de drogas, armas o de fraude bancario, portales de pornografía, posibilidad de contactar con sicarios, etcétera.

En relación con la red TOR, el nombre que se le ha asignado a este proyecto, The Onion Router, se debe a la estructura de nodos que utiliza para permitir la comunicación a la par que persigue el anonimato, dado que se compone de varias capas de cifrado, de manera similar a las capas que contiene una cebolla. Si bien no resultaría imposible conocer la procedencia de una cierta información transmitida a través de esta red, la existencia de distintas capas de cifrado dificulta en un amplísimo número de casos la posibilidad de determinar su origen o que pueda ser vinculada a un determinado autor.

Dentro de la red TOR uno de los servicios más utilizados es lo que se conoce como The Hidden Wiki, constituyendo un servicio realmente útil para todos aquellos usuarios que no sepan orientarse a través de esta red, dado que proporciona una especie de índice o directorio de páginas con extensión .onion a las que se puede acceder a través de TOR. Aun a pesar de todo, también resulta complejo localizar este recurso dentro de la red, puesto que, para garantizar la privacidad que tanto se persigue al introducirse en la Dark Web, el servidor y dominio que lo alojan es objeto de constantes modificaciones. Incluso, en ocasiones, es preciso obtener una invitación para acceder a The

Hidden Wiki, al igual que ocurre con muchos de los recursos que ofrece TOR.



- Logo de The Hidden Wikki-

En adición a lo anterior, cabe señalar que también existen réplicas de la información, al menos parcialmente, a la que se puede acceder a través de The Hidden Wiki desde Clearnet: <https://thehiddenwiki.org/>. En este sentido, dada la reciente popularidad de TOR, se han desarrollado pasarelas que también permiten el acceso a esta red sin la necesidad de instalar su software, como <https://www.onion.to/>.

Al igual que ocurre con The Hidden Wiki, existen otros recursos, si bien menos conocidos, que facilitan el acceso a los principales mercados, foros y buscadores de la Deep Web. Es el caso, por ejemplo, de IACA Dark Web Investigation Support Tool (<https://iaca-darkweb-tools.com/>), una herramienta gracias a la cual se puede comenzar a realizar cualquier investigación en la Internet Profunda. Para facilitar el acceso y el comienzo de cada investigación, una vez en TOR, esta página permite introducir términos de búsqueda en distintos buscadores conocidos como Not Evil, Torch, AHMIA, Onionland, DuckDuckGo o DeepLink y, una vez se pulsa en el botón correspondiente, hace aparecer ventanas emergentes que contienen los resultados de la búsqueda realizada para cada buscador que contiene la página. Incluso, posee un listado de mercados, foros y redes sociales conocidos que se

pueden visitar directamente eligiéndolos entre las opciones de un desplegable.

Entre otros, a través de la red TOR, al igual que a través de otro tipo de redes que permiten el acceso a la Deep Web, existe la posibilidad de acceder a distintos tipos de servicios, tanto legales como ilegales. Por mencionar algunos casos, existe la posibilidad de acceder a servicios de correo, que pueden ser tanto gratuitos como de pago; servicios de alojamiento y almacenamiento de archivos de dudosa legalidad y/o que contienen todo tipo de imágenes a las que no llega ningún límite legal, moral o de cualquier otra índole; servicios económicos y financieros en los que se trafica con datos bancarios, cuentas y tarjetas robadas, blanqueo de criptomonedas, falsificación de monedas y billetes, etcétera; servicios comerciales que proporcionan acceso al mercado negro, permiten realizar acciones de compraventa de cualquier tipo de droga, armas, documentación falsa o robada e incluso realizar actividades relacionadas con la explotación sexual; foros en los que se comenta o solicita información sobre cualquier aspecto, frecuentemente utilizados, entre otras cuestiones, para conectar a pederastas, distribuir pornografía infantil o solicitar información sobre las mejores drogas o formas para llevar a cabo un abuso sexual y salir impune; servicios de erotismo en los que no tiene cabida ningún tipo de límite o tabú; servicios dedicados al hacktivismo y al intercambio de documentos censurados; servicios de biblioteca en los que se puede acceder a una cantidad ingente de contenido, estén o no protegidos por copyright; servicios dedicados a la filtración de información altamente sensible procedente de entidades gubernamentales y distintos servicios de inteligencia, como Wikileaks; o servicios de contratación de ciberdelincuentes, en los que, a partir de 200 dólares, o menos según el caso, se podría ordenar la intrusión en un determinado sistema con cualquier finalidad, la realización de ataques de denegación de servicio en cualquiera de sus modalidades, la investigación a usuarios o incluso la obtención de sus perfiles y cuentas en redes sociales y servicios de correo, todo a cambio de un precio pactado previamente y pagado mediante criptomonedas, si bien ello no implica que el servicio vaya a

proporcionarse en la práctica y realmente constituya una estafa. En relación con esto último, a través de estos lugares del ciberespacio en ocasiones se ofrecen servicios de sicarios, en los que se publicitan y dan a conocer sus condiciones y sus límites, o la ausencia de ellos. En algunos casos, el precio por ordenar asesinatos ronda los 20.000 dólares, mientras que, si se desea que éste sea cometido con alguna condición específica como, por ejemplo, que se simule un accidente, podrían alcanzar los 75.000 dólares en el caso de una persona poco conocida o incluso superar los 300.000 en el caso de un alto cargo. Si bien es difícil acceder a un sitio concreto de la Deep web a no ser que se conozca la dirección .onion específica, resulta relativamente sencillo acceder a recursos que puedan promocionar cualquier tipo de actividad ilegal en la red sin tener la intención de hacerlo.

La reciente popularización de la red TOR incluso ha propiciado el desarrollo de una especie de buscador que trata de imitar a Google, tanto en su utilización como su apariencia, llegando a conocerse incluso como el “Google de la Dark Web”. Se trata de Grams, un buscador bastante sofisticado en el que, a partir de la introducción de algún término, encuentra resultados relacionados en los principales mercados negros existentes, siendo muy habitual su utilización para la obtención de acceso a mercados de droga. Irónicamente, el Google de la Dark Web dejó de estar operativo en 2017. Sin embargo, otras iniciativas y proyectos pasaron a sustituirlo, como Kilos, que desde hace alrededor de un año ha indexado más contenido del que llegó a almacenar nunca Grams.

CAPÍTULO II: CRONOLOGÍA Y EVOLUCIÓN DE LOS PRINCIPALES CIBERATAQUES DE LA HISTORIA

1.- Precedentes: el caso Blanc y los trabajos de Turing

El primer prototipo de ciberataque de la historia data del año 1834, hace casi doscientos años. Ocurrió en Francia, donde varias décadas atrás se había decidido construir la primera red nacional de datos: el telégrafo óptico. Este aparato estaba formado por una torre en cuyo tejado se instalaba un utensilio móvil de madera diseñado para verse a grandes distancias que permitía transmitir mensajes mediante la realización de movimientos que se correspondían con diferentes signos (letras y números). Los mensajes se enviaban a otras torres que recibían el mensaje observando el movimiento del utensilio mediante un telescopio, con lo cual a su vez replicaban el movimiento a lo largo de la red hasta la torre receptora del mensaje.

Aunque la utilización de la red estaba restringida a comunicaciones meramente gubernamentales, en el año 1834 los hermanos François y Joseph Blanc, banqueros de profesión,

descubrieron una manera de emplear el telégrafo para contribuir a sus propios intereses.

El primer paso consistió en sobornar a uno de los operadores del telégrafo en la ciudad de Tours para que introdujese mensajes ocultos en las comunicaciones rutinarias gubernamentales. Estos mensajes contenían información sobre los movimientos del mercado y el valor de los bonos del Tesoro francés, en cuyo comercio trabajaban los hermanos Blanc en la ciudad de Burdeos. La información tardaba en llegar varios días a esta localidad mediante los métodos convencionales de correo. De esta forma, al enterarse con antelación de los cambios de valor de los bonos, los hermanos Blanc conseguían grandes beneficios. Para conseguir la información, el operador del telégrafo introducía un carácter adicional al mensaje que debía transmitir y justo después efectuaba un signo que indicaba retroceso. Este signo servía para que el destinatario del mensaje ignorase el movimiento anterior cuando se hubiera producido una equivocación sin tener que volver a transmitir todo el mensaje desde el origen. El carácter que supuestamente se debía obviar en la comunicación en realidad aportaba información sobre el movimiento del mercado del día anterior.

El segundo paso consistió en sobornar a un antiguo operador de telégrafo que trabajaba en la torre de Burdeos y que se encargaba de interceptar el mensaje mediante la utilización de un telescopio. Éste, a su vez, transmitía las novedades diariamente a los hermanos Blanc.

Estas actividades fueron descubiertas dos años después al enfermar el cómplice en la ciudad de Tours de los hermanos Blanc, pues éste le desveló el acuerdo a su sustituto para que continuase su labor. Sin embargo, su compañero decidió revelar el trato a las autoridades, lo cual condujo al enjuiciamiento de los hermanos Blanc. No obstante, no llegaron a ser condenados debido a la ausencia de legislación en la materia.

Fue por la forma y el medio en el que se llevó a cabo, así como por las consecuencias legales y políticas que tuvo, por lo que se

consideró el primer ciberataque de la historia. Hizo visible la creciente necesidad de legislar acerca del uso fraudulento de los datos a través de los sistemas de comunicación que comenzaban a desarrollarse.

Sin embargo, el uso fraudulento del telégrafo dista mucho de lo que significa y de lo que implica un ciberataque hoy en día, teniendo en cuenta que se ha sustituido por dispositivos que permiten transmitir la información a tiempo real, así como que su uso se ha ido reduciendo con el tiempo hasta prácticamente desaparecer.

Algo más de un siglo después del ciberataque en Francia, ocurrió otro acontecimiento de trascendencia internacional que puso de relieve la importancia de la seguridad de la información. Aunque por sus características no se puede considerar un ciberataque, se debe mencionar que, en el año 1939, tras estallar la Segunda Guerra Mundial, se le encomendó al matemático Alan Turing, quien trabajaba para el Servicio de Inteligencia Británico, la tarea de descifrar el código secreto de la máquina criptográfica Enigma, que era utilizada por Alemania para asegurar la confidencialidad en sus comunicaciones militares.

Enigma era una máquina de cifrado con un grado de complejidad muy elevado. Contaba con un teclado en el que se introducía el mensaje que se quería cifrar y la máquina producía el mensaje de salida mediante un mecanismo con cinco rotores, intercambiando unas letras del mensaje por otras que no tenían un significado aparente. Lo que hacía que esta máquina fuese casi imposible de descifrar era que los rotores variaban cada vez que se pulsaba una tecla, de modo que era muy difícil establecer un patrón que indicase con qué signo se identificaba cada letra del alfabeto. Para añadir seguridad al aparato, el ejército alemán, además, alteraba la posición de los rotores cada mes.

Al comprender la complejidad de la operación, el servicio de inteligencia británico y el polaco comenzaron a cooperar para descifrar el código alemán.



- Máquina de cifrado Enigma-

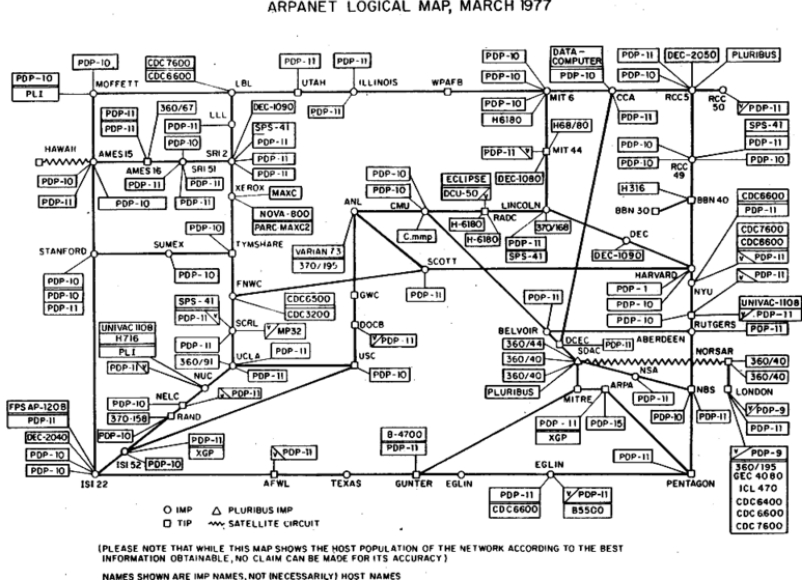
Tres meses después, Alan Turing pudo descifrar Enigma. Sin embargo, como el ejército alemán variaba los rotores una vez al mes manualmente y se empleaba mucho tiempo en descifrar Enigma cada vez, era imposible sacarle partido a la ventaja que había conseguido Turing. Por ese motivo, Turing diseñó un sistema automatizado que pasaría a llamarse “Bomba” y que tenía como objetivo predecir, mediante el cálculo matemático, las posiciones a las que se moverían los rotores. De esta forma reducían el abanico de posibilidades probando aquellas combinaciones que, según la máquina, eran más probables de aparecer.

Con el descifrado de las comunicaciones del ejército alemán, Reino Unido obtuvo una ventaja estratégica que fue determinante para concluir la guerra. Tanto es así que se ha estimado que redujo su duración en dos años. Gracias a Turing, Reino Unido fue capaz de frenar el avance de Alemania neutralizando un gran número de sus operaciones militares. Puede ser considerado, por tanto, el primer acto o la primera operación de ciber guerra de la historia, un acontecimiento que, si bien no coexistió con el entorno cibernético tal y como es entendido actualmente, puso de manifiesto que el uso de las tecnologías podía proporcionar una ventaja estratégica en la guerra, mediante el sabotaje de las comunicaciones o, lo que es lo mismo, con el robo o filtrado de información.

No obstante, como ya se ha señalado en los epígrafes anteriores, la ciberseguridad y el ciberespacio están relacionados en un alto grado con el surgimiento de las TIC y el desarrollo de Internet. Por tanto, el súbito desarrollo que han experimentado ha propiciado que no se pueda hablar de verdaderos actos de ciber guerra, ciberdelincuencia o ciberterrorismo, o, en general, de ciberataques, tal y como se les entiende actualmente hasta los últimos años del siglo XX y, especialmente, a partir del siglo XXI.

2.- Los primeros ciberataques

En el año 1971 se propagó el primer virus informático del que se tiene constancia. No obstante, era inofensivo, al igual que todos los virus que comenzaron a circular a partir de entonces, por lo que tampoco se puede tildar como el primer ciberataque de la historia. Conocido como Creeper (enredadera), fue desplegado sobre distintos ordenadores de ARPANET, propagándose a través de la red realizando copias de sí mismo y con una finalidad meramente molesta, pues su única funcionalidad consistía en difundir un mensaje en los ordenadores infectados que decía: *"I'm the Creeper, catch me if you can!"*.



-Mapeado de ARPANET-

Después de mostrar el mensaje se borraba del dispositivo infectado y procedía a difundirlo en otro ordenador. Teniendo en cuenta lo anterior, no tenía incorporada una funcionalidad dañina que permitiese calificarlo como un programa o software malicioso, no provocó la necesidad de modificar los estándares de la seguridad tales como se conocían ni de trasladar los existentes al ciberespacio, pero sí condujo al desarrollo del primer antivirus de la historia, otro virus, denominado Reaper, que se propagaba a través de la red con la finalidad de encontrar los ordenadores infectados con Creeper y eliminarlo de los sistemas afectados.

Tres años más tarde, en 1974, se identificó el primer virus informático diseñado con una finalidad maliciosa. Se trata de Rabbit, también conocido como Wabbit, un tipo de malware autorreplicable que mediante la realización de una cantidad ingente de copias de sí mismo dentro de un mismo equipo infectado podía provocar una reducción del rendimiento del dispositivo o incluso su colapso.

El malware fue objeto de un profundo desarrollo y proliferaron multitud de variantes con distintas finalidades, si bien todas mantenían una característica común, la producción de algún tipo de daño. El 2 de noviembre del año 1988, alrededor de una década más tarde, ocurrió el primer incidente de seguridad informática verdaderamente preocupante en la historia de la ciberseguridad. Morris, estudiante de la Universidad de Cornell e hijo de un empleado del departamento de seguridad informática de la NSA, desató, sin que aún hoy se tenga claro si fue de forma accidental o intencional, una poderosa amenaza que causó estragos sobre el 10% de los ordenadores conectados a Internet en ese momento. El gusano desplegado, que pasó a ser conocido por el nombre de la persona que lo creó, estuvo activo sobre los dispositivos infectados alrededor de 72 horas, durante las cuales pudo descargar archivos de distintos directorios de algunos de los dispositivos afectados y ejecutar procesos que ralentizaban el funcionamiento de los sistemas, llegando a paralizar las actividades que se estuviesen llevando a cabo y entorpeciendo su conexión durante varios días. La infección alcanzó a

varios organismos conectados a ARPANET, como la NSA, el MIT o el Pentágono. Además, ocasionó pérdidas económicas por valor de entre cien mil y diez millones de dólares. Morris, el desarrollador de este gusano, fue la primera persona condenada por realizar un delito informático relacionado con el desarrollo y propagación de malware.

Así mismo, en relación con otro de los primeros ciberataques que provocó un alto impacto, es preciso mencionar el gusano I Love You, un tipo de malware desarrollado en VBScript, desplegado durante el mes de mayo del año 2000, que llegó a propagarse sobre más de cincuenta millones de ordenadores alrededor de todo el mundo, afectando incluso a instituciones altamente securizadas como el Pentágono, la CIA o el parlamento británico. La idea era simple: los atacantes enviaban un mensaje de correo electrónico con el asunto “I Love You” a los destinatarios y con un archivo adjunto con extensión .vbs que simulaba constituir una carta de amor del remitente. En los casos en los que el destinatario trató de leer el archivo adjunto, en realidad se ejecutaba un script que permitía la infección del dispositivo con el virus. Además, utilizaba la libreta de direcciones del usuario infectado y su dirección de correo electrónico para reenviar el mensaje a todos sus contactos e incrementar su capacidad de propagación. I Love You fue desarrollado por Onel de Guzmán, un individuo de origen filipino, conocido en la red como Spyder, que consiguió provocar pérdidas millonarias, pues el virus instalaba un troyano en los dispositivos afectados con la funcionalidad de destruir la información almacenada en el disco duro, incluyendo la eliminación de ficheros con extensiones .vbs, .vbe, .js, .jse, .css, .wsh, .sct, .hta, .jpg y .jpeg y su sustitución por copias del virus.

En 2001 hubo otro ciberataque que adquirió importancia mediática. Fue el caso del gusano Code Red, un tipo de malware diseñado para operar en entornos con Windows, desplegándose sobre los dispositivos mediante la explotación de una vulnerabilidad que afectaba a Microsoft. Code Red trataba de desplegarse en el mayor número posible de servidores web Internet Information Server 5.0 (IIS),

de modo que una vez lo hubo conseguido utilizó los dispositivos infectados para lanzar un gran número de peticiones contra la página web de la Casa Blanca y conducir al sitio web a una denegación de servicio.

3.- La eclosión de los ciberataques

Como se ha podido comprobar, hasta el momento los ciberataques que tuvieron lugar eran bastante simples y revestían escasa complejidad y preparación. En la mayor parte de las situaciones no estaban dirigidos hacia una organización o sector en concreto y en los casos en los que sucedía no provocaba un alto impacto.

Durante el periodo que aconteció después tuvieron lugar otra serie de ciberataques aislados contra objetivos como:

- La NASA, que tuvo que bloquear en diciembre de 2006 la recepción de correos electrónicos con archivos adjuntos ante la posibilidad de que se produjese un hackeo después de que varios actores desconocidos realizasen una intrusión en sus sistemas y obtuviesen los planes de lanzamiento de transbordadores espaciales.

- La administración telemática del gobierno de Estonia, que fue víctima de un ataque de denegación de servicio en abril de 2007, después de que tuviese lugar una discusión entre Estonia y Rusia relacionada con la destrucción de un monumento de guerra.

- El Pentágono, que en junio de 2007 tuvo que contener un intento de intrusión después de que la dirección de correo no clasificada del secretario de defensa de Estados Unidos fuera comprometida.

- El Ministerio de Seguridad de China, que detectó en octubre de 2007 que distintos actores procedentes mayoritariamente de Taiwán y Estados Unidos habían estado robando información de sectores importantes del estado.

- Las elecciones estadounidenses, que durante la campaña electoral de 2008 fueron objeto de un ciberataque que concluyó con la adquisición no autorizada de las bases de datos de los partidos demócrata y republicano por actores extranjeros desconocidos.

- El gobierno de Georgia, cuyas redes fueron víctima de un ciberataque en agosto de 2008 debido al cual los sitios web de la administración fueron objeto de un *defacement*, en el marco de una disputa entre la nación y Rusia.

- El gobierno de Israel, cuyos sitios web fueron desestabilizados en enero de 2009 por la acción conjunta de alrededor de cinco millones de ordenadores, con motivo de la ofensiva militar lanzada sobre la Franja de Gaza, especulándose acerca de la posible participación de organizaciones criminales vinculadas a Rusia y financiadas por Hamas o Hezbollah.

- El motor de búsqueda chino Baidu, que, en enero, de 2010 fue comprometido y utilizado por un grupo que se autodenominaba Iranian Cyber Army para redirigir a los usuarios a una página web que contenía un mensaje político iraní.

En algunos casos los ciberataques fueron frustrados antes de que pudieran ocasionar algún tipo de impacto y en otros este pudo solventarse con relativa facilidad. Todos ellos constituían ciberataques que empezaban a denotar la importancia que iba adquiriendo poco a poco la ciberseguridad, la necesidad de proteger unos medios telemáticos cada vez más utilizados no solo por usuarios individuales,

sino también por empresas y organismos tanto del sector público como privado.

La generalización del uso de las TIC provocó que distintos tipos de actores (cibercriminales, hacktivistas, grupos de actores especializados en la realización de amenazas persistentes avanzadas y/o respaldados por algún estado-nación, etcétera) trasladasen su actividad al entorno virtual, de manera que los ciberataques iban haciéndose, poco a poco, más complejos y sofisticados.

4.- Stuxnet

Si hubo un ciberataque que supuso un verdadero cambio de paradigma y puso de manifiesto la necesidad de promover una cultura de ciberseguridad fue Stuxnet, un malware de la categoría gusano que en el año 2010 fue introducido en la central nuclear iraní de Natanz y llegó a infectar mil máquinas utilizadas para la producción de materiales nucleares.

El impacto provocado por Stuxnet se hizo notorio por primera vez durante el mes de enero del año 2010, cuando varios inspectores de la Agencia Internacional de Energía Atómica visitaron la planta nuclear de Natanz y notaron que las centrifugadoras utilizadas para enriquecer el uranio no funcionaban con normalidad, a pesar de que en ese momento se debió tratar como un fallo puntual, puesto que el incidente no fue objeto de un examen profundo. Sin embargo, cinco meses más tarde, en junio del año 2010, volvió a detectarse un comportamiento anómalo en las centrifugadoras. Por suerte, en este momento los trabajadores de la central pudieron identificar la causa del fallo.

Al descubrir la existencia de Stuxnet, los analistas que se encargaban de su investigación comprobaron que se trataba de un malware muy complejo y que había sido diseñado con una finalidad

bélica. Por tanto, significó la detección de la primera ciberarma de la historia.

Se descubrió que Stuxnet había infectado una de las máquinas de la central a través de un dispositivo USB en el que había sido almacenado previamente. Posteriormente, se propagó por la red y las impresoras compartidas, hacia el resto de máquinas. Stuxnet fue programado específicamente para observar cómo operaban los sistemas de la central y registrar los datos, así como para apuntar y destruir las centrifugadoras. Para conseguir que las centrifugadoras se deteriorasen este malware alteraba repentinamente la velocidad de sus rotores. Además, reproducía los datos que indicaban un funcionamiento normal en la maquinaria para que los empleados no se diesen cuenta de la infección. Gracias a ello Stuxnet consiguió paralizar la producción de uranio enriquecido durante casi tres años en la central nuclear de Natanz.

Aunque no existen datos oficiales sobre el origen de Stuxnet, se tienen sospechas considerables acerca de que fuera desarrollado y distribuido por la inteligencia israelí y la estadounidense, en un intento por retrasar el programa nuclear iraní, y lo consiguieron durante años.

Por primera vez en la historia, un ciberataque logró dañar e incluso causar estragos sobre la infraestructura del mundo real. Por tanto, no solo se trata de la creación de una nueva ciberarma, sino del primer acto deliberado de ciberguerra de la historia, un acontecimiento bélico producido en un contexto que trasciende del entorno físico. Se trata, también, de la primera amenaza persistente avanzada (APT) de la historia.

Stuxnet dio a conocer el peligro que suponía no proteger los dispositivos conectados a la red y, en especial, las infraestructuras críticas, cuyo deterioro podía llegar a paralizar un país. Con anterioridad a este hecho no había salido a la luz ningún malware con capacidades destructivas similares, sino que, tal y como se expuso con

anterioridad, eran muy comunes los virus que, en el peor de los casos, dejaban inoperativos algún que otro archivo dentro del dispositivo; o, en casos aislados, alguna filtración de datos, como principales amenazas a la seguridad informática.

5.- Entre Stuxnet y WannaCry

A la par que el concepto de ciberguerra comenzaba a ocupar un lugar específico dentro de la sociedad, el concepto de cibercriminalidad también. En este sentido, comenzaron a proliferar distintos grupos de actores que operan en el ciberespacio y emprendieron una especialización sostenida en la ejecución de campañas de ciberataques basadas en la utilización de amenazas persistentes avanzadas (APT).

Uno de los grupos de actores avistados que alcanzó relevancia en el escenario internacional después del desastre de Stuxnet fue Red October, una red de ciberespionaje que operaba principalmente en la zona de Europa del Este y Asia Central. Dada a conocer en 2013, la campaña iniciada por este grupo se remonta al año 2007, siendo bastante habitual que las campañas de ciberespionaje tarden meses o incluso años en ser identificadas, pues tratan de recabar datos e información durante el máximo periodo de tiempo posible y, en consecuencia, de evadir su detección.

Red October se dirigía a objetivos gubernamentales, entidades diplomáticas y organizaciones de investigación científica, con la finalidad de recabar información de alto valor procedente de estos sectores, para lo cual, por lo general, desarrollaba o utilizaba exploits ya existentes que permitiesen aprovechar vulnerabilidades conocidas en Office y, en menor medida, Java, incrustados en archivos adjuntos que enviaban a sus potenciales víctimas a través del correo electrónico y que contenían la carga útil que realizaba la labor de monitoreo. Además, el malware empleado durante el transcurso de la campaña permitía recopilar datos no solo de ordenadores, sino también de otros

dispositivos como teléfonos móviles, equipos de red empresarial y unidades de disco extraíbles.

Por otro lado, en 2013 ocurrió otro acontecimiento de suma importancia en el panorama de la ciberseguridad a nivel global. El motor de búsqueda Yahoo! fue víctima de un importante ciberataque, conocido aun actualmente como el mayor robo de datos a usuarios que ha tenido lugar hasta la fecha. Un grupo de cibercriminales, sobre los que se sospecha que podrían estar respaldados por algún estado o nación, provocó una fuga masiva de los datos contenidos en los servidores de este popular portal que afectó a la totalidad de sus usuarios, es decir, más de tres mil millones de individuos, si bien las investigaciones iniciales indicaron que la cifra total de afectados rondaba los quinientos millones de cuentas y no pudo conocerse el número real de perfiles comprometidos hasta el año 2016.

Entre los datos expuestos había tanto nombres de usuarios como nombres reales de las personas propietarias de las cuentas, así como sus direcciones de correo electrónico, sus contraseñas, números de teléfono, conversaciones, fechas de nacimiento y preguntas de seguridad, entre otros.

Después de que se produjese la filtración, Yahoo!, que fue adquirida por Verizon, comenzó a contactar con sus usuarios para dar a conocer el alcance de la filtración y solicitar que cambiaran sus credenciales, preguntas de seguridad y demás mecanismos destinados a proteger sus datos personales y sus cuentas de usuario.

Al año siguiente tuvo lugar el mayor ciberataque soportado por una entidad empresarial estadounidense. En el año 2014, el grupo de actores Lazarus, también conocido como *Guardians of the Peace*, *Dark Seoul*, *Hidden Cobra*, *Hastati Group*, *Andariel*, *Unit 121*, *Bureau 121*, *NewRomanic Cyber Army Team*, *Bluenoroff*, *Group 77*, *Operation Troy* o *Operation GhostSecret* entre otros alias y vinculado a Corea del Norte, lanzó un ciberataque sobre los sistemas de Sony Pictures,

consiguiendo paralizar su actividad y ocasionando una fuga masiva de datos confidenciales, registros financieros y correos electrónicos privados de ejecutivos de Hollywood. Incluso, llegaron a filtrarse varias películas que todavía no habían sido estrenadas en cartelera y guiones de largometrajes que debían rodarse próximamente, además de información personal y laboral de los empleados de Sony Pictures, que fueron amenazados por el grupo, así como datos e información personal de varios actores que trabajaban en las películas de la entidad.

En el momento en el que la entidad se percató del ciberataque, bloqueó los accesos a sus redes informáticas y las desconectó de Internet, con la finalidad de paralizar la intrusión, circunstancia que impidió el normal funcionamiento de la compañía durante varios días. Además, análisis posteriores permitieron descubrir que Sony Pictures había sido infectada con el gusano Wiper, un tipo de malware con la capacidad de dejar inoperativos los sistemas mediante la sobreescritura de sus unidades de disco.

Se estima que el grupo obtuvo alrededor de 100 terabytes de información sensible y que dicho ciberataque ocasionó pérdidas por un valor superior a 200 millones de dólares a la compañía. Curiosamente, se dictaminó que la causa del ataque fue el estreno de la película “The Interview”, película en la que se intentaba asesinar al líder norcoreano Kim Jong-un. Tras el ataque, la compañía canceló el estreno puesto que recibieron varias amenazas de ataques terroristas.



WANTED BY THE FBI

PARK JIN HYOK

**Conspiracy to Commit Wire Fraud; Conspiracy to Commit Computer-Related Fraud
(Computer Intrusion)**



DESCRIPTION

Aliases: Pak Jin Hek, Jin Hyok Park

Place of Birth: Democratic People's Republic of Korea (North Korea)

Hair: Black

Eyes: Brown

Sex: Male

Race: Asian

Languages: English, Korean

REMARKS

Park attended the Kim Chaek University of Technology in Pyongyang, North Korea. He is a North Korean citizen last known to be in North Korea. Park has traveled to China in the past and conducted legitimate IT work under the front company "Chosun Expo" or the Korean Expo Joint Venture in addition to activities conducted on behalf of North Korea's Reconnaissance General Bureau.

CAUTION

Park Jin Hyok is allegedly a North Korean computer programmer who is part of a state-sponsored hacking organization responsible for some of the costliest computer intrusions in history, including the cyber attack on Sony Pictures Entertainment, a series of attacks targeting banks across the world that collectively attempted to steal more than one billion dollars, and the WannaCry ransomware attack that affected tens of thousands of computer systems across the globe.

Park was alleged to be a participant in a wide-ranging criminal conspiracy undertaken by a group of hackers employed by a company that was operated by the North Korean government. The front company - Chosun Expo Joint Venture, also known as Korea Expo Joint Venture - was affiliated with Lab 110, one of the North Korean government's hacking organizations. That hacking group is what some private cybersecurity researchers have labeled the "Lazarus Group." On June 8, 2018, a federal arrest warrant was issued for Park Jin Hyok in the United States District Court, Central District of California, after he was charged with one count of conspiracy to commit wire fraud and one count of conspiracy to commit computer-related fraud (computer intrusion).

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Los Angeles

- Cartel de "se busca" por el FBI de un presunto miembro de Lazarus-

Ese mismo año tuvo lugar otro de los ciberataques que salpicó a la industria del cine y supuso un escándalo relacionado con el panorama hollywoodense. Celebgate, nombre que se otorgó a la campaña, consistió en una serie de ciberataques contra distintas celebridades, como Jennifer Lawrence, Scarlett Johanson o Kirsten Dunst, que concluyó con la divulgación pública de sus fotografías íntimas en varios lugares de Internet como distintos portales de pornografía con mujeres famosas, después de que los ciberdelincuentes intentasen sin éxito lucrarse con ellas. La campaña tuvo dos puntos álgidos en los años 2011 y 2014, si bien aun actualmente continúan dándose casos relacionados con esta operación, a pesar de que sus precursores fueron procesados judicialmente.

Los ciberdelincuentes que llevaron a cabo esta campaña, que no parecían estar relacionados entre sí, obtuvieron las fotografías gracias a la explotación de vulnerabilidades en los servicios de almacenamiento en la nube iCloud de Apple y Gmail de Google y a la utilización de técnicas de ingeniería social, solicitando a las víctimas los datos de acceso a esos servicios en alguna comunicación que aparentase provenir del proveedor en cuestión.

Continuando con las campañas de filtraciones de datos, en el año 2015 el portal web de citas extramatrimoniales Ashley Madison fue víctima de una violación de datos a consecuencia de la cual se publicaron en línea los datos de 37 millones de usuarios de la página. La filtración, realizada por un grupo de actores que se autodenominaba The Impact Team, consistía en una forma de protesta contra la entidad y la empresa gestora de éste y otros portales similares, ALM, debido a que el grupo de ciberactores consideraba que los datos de sus clientes no estaban debidamente protegidos. Concretamente, querían probar que la opción “hard-deleted”, concebida para borrar todo rastro de la actividad en el sitio, no funcionaba según lo esperado, a pesar de constituir una funcionalidad de pago. A consecuencia de lo anterior, los ciberdelincuentes exigían a la empresa el cierre inmediato de Ashley Madison y de otro de sus portales o, de lo contrario, filtrarían la

totalidad de la información que habían recopilado durante el transcurso de la campaña, entre cuyos datos se encontraban los nombres y direcciones reales de los usuarios, sus perfiles, sus preferencias y fantasías sexuales, las operaciones que habían realizado utilizando una tarjeta de crédito, sus datos bancarios, direcciones de correo, etcétera.

Un mes después, fecha del vencimiento otorgado por los atacantes, al comprobar que ALM no había accedido a sus demandas, The Impact Team publicó los datos en la Dark Web. Este ciberataque supuso no solo la salida del director ejecutivo de la compañía, sino que además suponía implicaciones muy graves para cada uno de sus usuarios, dado que al ser filtrados datos tan sensibles podían ser objeto tanto en el presente como en el futuro de múltiples fraudes, chantajes y extorsiones.

Otro de los acontecimientos más importantes que tuvo lugar durante el año 2015 en relación con el panorama de la ciberseguridad fue una filtración masiva de datos de la empresa de seguridad italiana Hacking Team, una organización dedicada al desarrollo de herramientas de vigilancia y software espía para cuerpos y fuerzas de seguridad del estado de distintos países. Entre los 400 gigabytes de información recabada por los atacantes, los cuales fueron publicados para su descarga en Torrent, había mensajes de correo electrónico internos de la compañía, el listado de países a los que proveían con sus herramientas de spyware y los datos de las transacciones realizadas a tal efecto, etcétera.

Lo más controvertido de todo fue que, incluso, llegó a filtrarse el código fuente de la herramienta de spyware Da Vinci, un troyano capaz de recabar todo tipo de información del dispositivo afectado, como mensajes de chat, llamadas de Skype, documentos, contraseñas, etcétera. Los ciberdelincuentes que llevaron a cabo este ciberataque también obtuvieron acceso al perfil oficial de Twitter de la entidad e hicieron publicidad de las filtraciones a través de ese canal, cambiando su nombre oficial, Hacking Team, por Hacked Team.

En relación con los países que habían llegado a un acuerdo comercial con esta empresa italiana estaba España, que habría firmado un contrato con ellos a través del CNI para obtener acceso a herramientas que permitiesen espiar las telecomunicaciones y otorgasen acceso a dispositivos móviles y ordenadores, si bien Hacking Team argumentó que las herramientas solo eran utilizadas en investigaciones delicadas y graves relacionadas con el terrorismo, la pederastia y la criminalidad organizada. Entre sus clientes había estados pertenecientes a casi todos los continentes, incluyendo Estados Unidos, Alemania, Rusia o Corea del Sur, entre muchos otros, e incluso regímenes represores como Sudán, circunstancia que dio lugar a un conflicto social al dar cuenta de que Italia proporcionaba soporte a regímenes dictatoriales.

En el mes de agosto del año 2016 se produjo otra violación de datos sobre una gran empresa de seguridad, nada menos que la Agencia Nacional de Seguridad de Estados Unidos (NSA). El grupo cibercriminal y hacktivista The Shadow Brokers, desconocido hasta entonces, realizó una intrusión en los sistemas de Equation Group, una organización dedicada a la ejecución de operaciones principalmente relacionadas con el ciberespionaje y vinculada a la NSA, gracias a lo cual obtuvo varias herramientas de espionaje, exploits y distintos tipos de software que posibilitaban el acceso a prácticamente cualquier sistema. En un primer momento, el grupo cibercriminal The Shadow Brokers decidió poner a la venta la información supuestamente obtenida de los sistemas informáticos de la NSA por un valor de 10.000 bitcoins, lo que equivaldría a alrededor de 25 millones de euros. Sin embargo, no pareció suscitar expectación y no obtuvieron compradores, circunstancia que provocó que el grupo filtrase en un repositorio de GitHub una parte de las herramientas robadas, lo que puso en jaque a la ciberseguridad tal y como se conoce actualmente, puesto que gracias a esa filtración tuvieron lugar algunos de los mayores ciberataques que se han producido en la historia.



-Sede la NSA en Fort Meade, Maryland-

Teniendo en cuenta el interés originado tras la filtración original, durante el año 2016 y el año 2017 The Shadow Brokers continuó poniendo a la venta las herramientas robadas y filtrando parte de ellas en el ciberespacio. Entre las herramientas filtradas podía encontrarse el código de Stuxnet, así como distintos tipos de spyware dirigidos a productos de proveedores como Cisco, Juniper, Fortigate y Topsec. Sin embargo, el mayor impacto, tanto a nivel de repercusión mediática como por el daño que llegaron a producir, fue atribuido a la divulgación de los exploits EternalBlue, EternalRomance y DoublePulsar, diseñados para aprovechar vulnerabilidades en una gran variedad o incluso todas las versiones de Windows con la finalidad de otorgar acceso en remoto a los posibles atacantes que las empleasen.

6.- WannaCry

En el año 2017 las filtraciones de datos continuaron teniendo lugar, pero fueron relegadas a un segundo plano por una amenaza, si cabe, mayor, el ransomware. El 12 de mayo de 2017 se produjo el mayor ciberataque de ransomware de la historia. Conocido como WannaCry, llegó a afectar a alrededor de 300.000 máquinas distribuidas entre más de 150 países.

En España la primera organización afectada por esta campaña masiva de ciberataques fue Telefónica, lo que condujo a pensar que podía ser un ataque dirigido contra esta empresa de telecomunicaciones. Sin embargo, se trataba de un ciberataque indiscriminado que sobrepasó por completo cualquier barrera nacional.

Los países más perjudicados por WannaCry fueron Rusia, Ucrania y la India. En Rusia se vieron afectados los servicios de los centros de atención telefónica y una parte de los puntos de venta. El Ministerio del Interior ruso también fue infectado por el ransomware y la policía no pudo expedir permisos de conducir ni matrículas de automóviles. También se vieron afectados por WannaCry el Ministerio de Sanidad, las entidades bancarias y los servicios de ferrocarriles. En Ucrania se vio afectado su aeropuerto más grande, en Kiev, por lo que los vuelos fueron retrasados, y su servicio de metro, imposibilitándose la compra de billetes. También infectó los dispositivos de su Banco Central, de la compañía estatal de energía y la red informática del Gobierno. En la India resultaron afectados los sistemas informáticos de la policía.



- Pantalla generada por WannaCry-

Por otro lado, en China distintas universidades también fueron víctimas de este ransomware y los trabajos de fin de grado de los alumnos fueron cifrados, lo que provocó que muchos se vieran obligados a pagar el rescate para poder presentarlos. En Corea del Sur WannaCry afectó a la mayor cadena de cines del país, aunque no se paralizó la proyección de películas.

En España tuvo incidencia, como ya se ha señalado, sobre Telefónica, además de Iberdrola y Gas Natural. En Francia, Renault tuvo que paralizar la producción de automóviles porque el ciberataque también alcanzó sus filiales locales, así como las ubicadas en Eslovenia y Rumanía. En Alemania también se vio afectada por WannaCry la empresa ferroviaria Deutsche Bahn AG. En este caso las pantallas de

información para los pasajeros colocadas en las estaciones de tren fueron secuestradas por el ransomware.

Teniendo en cuenta lo anterior, se puede afirmar que WannaCry tuvo un impacto devastador, incluso llegó a afectar a 61 hospitales y centros de salud en Reino Unido, que fueron paralizados por completo a consecuencia de este ciberataque sin precedentes, de modo que se produjeron demoras en la atención a los pacientes y en muchos casos ni siquiera se les pudo atender. WannaCry infectó una gran cantidad de ordenadores y cifró toda la información que contenían sobre los pacientes de los centros afectados, como sus direcciones, sus teléfonos e historiales médicos, que eran inaccesibles en muchos hospitales. Los hospitales incluso se vieron obligados a desviar a sus pacientes a otros centros ante la imposibilidad de acceder a sus sistemas informáticos y coordinar la llegada de ambulancias y enfermos, así como ordenar la suspensión del tratamiento de los pacientes y cancelar alrededor de 7000 consultas. WannaCry también afectó a las máquinas en las que se almacenaban y refrigeraban las muestras de sangre y a los dispositivos electrónicos de los quirófanos y de radiología.

Este ciberataque puso de manifiesto las consecuencias que podía tener una campaña de este tipo, paralizando servicios básicos como la sanidad y trascendiendo de las barreras nacionales. Gran parte de las entidades afectadas dieron la orden a sus empleados de apagar y desconectar de la red todos los dispositivos para evitar la propagación del ransomware, lo que a su vez impidió en muchos casos que pudieran operar y ofrecer sus servicios con normalidad.

Este ransomware aprovechaba una vulnerabilidad crítica presente en dispositivos Windows que daba acceso a los atacantes a los dispositivos afectados para ejecutar código de forma remota, es decir, desde un lugar distinto al que se encontrase el dispositivo. Para conseguirlo, hacía uso del exploit EternalBlue, filtrado, al menos supuestamente, por el grupo The Shadow Brokers del arsenal de herramientas de la NSA. Aunque la vulnerabilidad había sido

solucionada por Microsoft dos meses antes de la propagación de WannaCry, millones de usuarios omitieron la actualización del sistema, bien por dejadez, por desconocimiento o por los largos tiempos de espera que requieren las actualizaciones, circunstancia que los hizo vulnerables frente al ataque. WannaCry estaba diseñado para que en el momento en el que se produjera el secuestro del dispositivo apareciese un mensaje en el aparato que exigía un rescate pecuniario (300 dólares a una cuenta de bitcoin) a cambio de recuperar el acceso al sistema.

Posteriormente las investigaciones se centraron en descubrir quién o quiénes habían sido los responsables del desarrollo y la distribución de WannaCry. Lo primero que se descubrió fue que el ciberataque procedía de Corea del Norte. A partir de ahí, gracias al análisis del código de WannaCry y sus similitudes con otros tipos de malware que había creado el grupo anteriormente, se pudo vincular su creación y distribución al grupo de actores Lazarus, el mismo al que se atribuyó la responsabilidad del ciberataque a Sony Pictures.

A pesar de que se vieron afectados más de 300.000 dispositivos por el ciberataque global de WannaCry, se calcula que Lazarus se hizo con menos de 70.000 dólares (63.774 euros) por los rescates para recuperar sus datos. Sin embargo, ninguna de las entidades que pagaron el rescate recuperaron los datos cifrados. Otros investigadores calculan que los atacantes pudieron hacerse con alrededor de 140000 dólares en monedas virtuales (bitcoin), en cualquier caso, una cifra baja. Por tanto, o bien el ataque fue poco efectivo para los atacantes, puesto que en otras ocasiones habían podido hacerse con cantidades monetarias ingentes, como con el ataque al Banco Central de Bangladesh de 2016, o bien su motivación no era solamente de índole económica, sino que aspiraba, presumiblemente a algún tipo de finalidad corporativa o política, dos de los motivos principales por los que actúan los actores respaldados por algún estado o nación.

Este ransomware fue neutralizado gracias a la labor de Marcus Hutchins, un hacker de 22 años al momento de la infección que encontró un fallo en el código de desarrollo de WannaCry, que servía como medida de desactivación del ataque. Curiosamente, el héroe de WannaCry fue después detenido por haber desarrollado otro malware, Kronos, que afectaba exclusivamente al sector bancario, pero finalmente ha sido absuelto por su colaboración en el caso WannaCry.

7.- NotPetya

Aún recuperándose del impacto devastador de WannaCry, el escenario internacional se vio estremecido poco después por otro ciberataque catastrófico. Denominado por la mayoría de investigadores como NotPetya y conocido por algunos como WannaCry 2.0, es una variante del ransomware Petya, un tipo de malware detectado en el año 2016 que se distribuía mediante el envío de mensajes de correo electrónico incrustado dentro de archivos maliciosos adjuntos.

La variante NotPetya, que abarcaba tanto funcionalidades de ransomware como de gusano, fue distribuida durante el transcurso de un ciberataque que comenzó en el mes de junio del año 2017, apenas un mes después de la propagación de WannaCry. El ciberataque se detectó por primera vez en Ucrania, afectando a una entidad en Kiev. Rápidamente se propagó por todo el país, perturbando las actividades del Banco Nacional del estado, donde fue especialmente dañino, del gobierno, de la compañía estatal de electricidad, del metro y de un aeropuerto de Kiev, del servicio estatal de correos, de diferentes empresas operadoras de telefonía fija y móvil, de las fuerzas y cuerpos de seguridad del estado, así como distintas cadenas de televisión y distintos medios informativos.



- Imagen que mostraba en pantalla la primera versión de Petya-

No obstante, aunque constituyó el epicentro del ciberataque, no solo Ucrania fue golpeado por NotPetya, sino que se propagó por Estados Unidos, afectando a la mayor empresa farmacéutica de la nación, y distintos países de Europa. Además, tuvo especial incidencia en Rusia, donde llegó a afectar a algunas de las mayores empresas petroleras y siderúrgicas de la nación, Reino Unido, afectando a la mayor empresa de publicidad a nivel internacional, WPP, y la India, afectando a sus puertos principales y a empresas de administración de propiedades e inversiones. En relación con otros países, también se detectó afectación sobre la empresa danesa de transporte marítimo Moller-Maersk y varias entidades con sede en España como Saint Gobain, dedicada a la fabricación de materiales de construcción, DLA Piper, dedicada a la abogacía, y Mondelez Internacional, dedicada a la comercialización de bebidas, confitería y productos alimentarios.

Según dieron a conocer distintos investigadores, NotPetya utilizaba el mismo método de propagación que WannaCry, la explotación de una vulnerabilidad en Windows que, aun habiendo sido parcheada por el fabricante, no había sido aplicada por multitud de usuarios. En este caso también pareció hacerse uso de EternalBlue, una de las herramientas de exploit de la NSA filtrada por Shadow Brokers, al igual que ocurrió con WannaCry, así como del exploit EternalRomance, que utiliza el puerto TCP 445 y herramientas como psexec para ejecutar comandos en las máquinas a las que se conecta. No obstante, investigaciones posteriores revelaron que NotPetya también era distribuido mediante archivos ofimáticos de Excel y Word que aprovechaban una vulnerabilidad existente en Office y a la que se asignó el identificador CVE-2017-0199, así como mediante mensajes de correo electrónico de phishing que contenían enlaces maliciosos que permitían el despliegue del ransomware, que posteriormente trataba de infectar otros dispositivos conectados a la red local.

Una de las características de NotPetya, que lo diferenciaba de WannaCry era su capacidad para cifrar el Master File Table (MFT) del disco duro, una base de datos en la que se almacena información sobre cada archivo y directorio, lo que conduce a que el Master Boot Record (MBR), es decir, el registro de arranque maestro, quede inoperativo, reemplazándolo con el malware e incluyendo la nota de rescate: los atacantes solicitaban 300 dólares en bitcoins a cambio de la clave de descifrado, si bien no parecía constituir la finalidad primaria del ataque, al igual que con WannaCry. Además, el actor detrás del ataque perdió el acceso al correo electrónico con el que se comunicaba con las víctimas para proporcionar, supuestamente, las claves de descifrado, puesto que el proveedor de correo cerró la cuenta de los atacantes.



En los días posteriores al ataque Ucrania señaló, al igual que muchos investigadores de seguridad de distintos países, a Rusia como responsable de la campaña, indicando que su finalidad no era otra que desestabilizar a la nación y la actividad de distintas organizaciones públicas y privadas. Sin embargo, teniendo en cuenta que Rusia también figuró entre los objetivos de esta campaña de ransomware, las acusaciones fueron desmentidas por el estado. Incluso hoy, cuesta esclarecer la atribución y el objetivo del ciberataque NotPetya.

CAPÍTULO III

FORMAS DE LUCHAR CONTRA LAS AMENAZAS A LA SEGURIDAD INFORMÁTICA

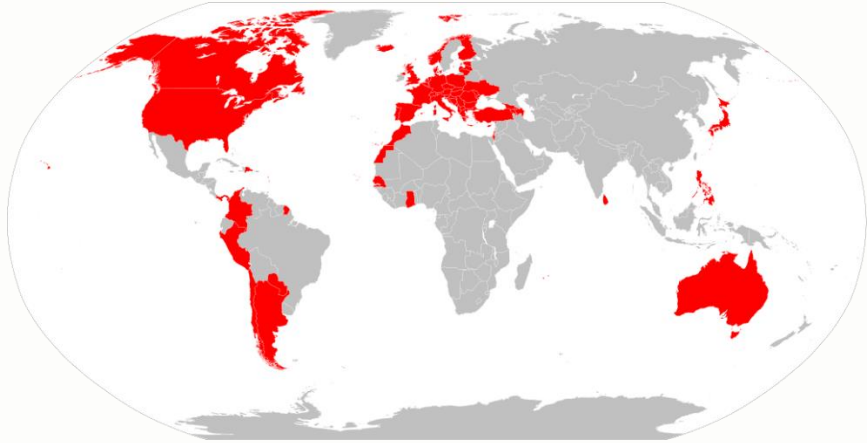
1.- Legislación supranacional

Al igual que ocurriría con cualquier otra clase de delito, el nuevo paradigma que supone la ciberseguridad implica la necesidad de desarrollar una nueva legislación que ampare este nuevo escenario, tanto a través de la creación de mecanismos de prevención como de organismos competentes para perseguir e investigar los delitos que puedan producirse en el ciberespacio, que deben actuar bajo los preceptos legales correspondientes.

Esta nueva necesidad de legislar acerca de un ámbito que hasta hace poco tiempo no tenía cabida en la sociedad se ha ido implementando paulatinamente en las Estrategias Nacionales de Seguridad de cada país, haciéndose hueco en las normativas que, tradicionalmente, versaban sobre escenarios muy diferentes al del ciberespacio, tales como las amenazas relacionadas con las

disfunciones de la globalización, los desequilibrios demográficos, la inestabilidad, pobreza y desigualdad en la sociedad, el cambio climático o la proliferación de ideologías radicales y no democráticas. Con el tiempo, también se han desarrollado normativas específicas relacionadas con la ciberseguridad tanto a nivel nacional como internacional.

La primera normativa que conviene destacar a nivel supranacional es el Convenio de Budapest, también conocido como Convenio sobre la Ciberdelincuencia, elaborado por el Consejo de Europa en Estrasburgo y firmado el 23 de noviembre de 2001 en Budapest por una gran cantidad de países. Concretamente, fueron 30 los países que firmaron el acuerdo: Albania, Alemania, Armenia, Azerbaiyán, Bosnia y Herzegovina, Bulgaria, Croacia, Chipre, Dinamarca, Eslovaquia, Eslovenia, España, Estados Unidos, Estonia, Finlandia, Francia, Hungría, Islandia, Italia, Letonia, Lituania, Antigua República Yugoslava de Macedonia, Montenegro, Noruega, Países Bajos, Portugal, República de Moldavia, Rumanía, Serbia y Ucrania.



- Firmantes del Convenio de Budapest-

El Convenio de Budapest supuso el primer tratado internacional que abordaba la reciente problemática causada por la necesidad de regulación de los posibles usos fraudulentos que pudiesen tener lugar en el ciberespacio. Como ya se ha comentado, España fue uno de los países firmantes, no obstante, la decisión no fue ratificada hasta el 1 de octubre de 2010, momento en el que la normativa entró en vigor. En el convenio se abordaron ciertos aspectos básicos de la terminología, así como las medidas que debían incorporarse a nivel nacional en relación con el derecho penal sustantivo, en el que se debían regular el acceso ilícito, la interceptación ilícita, la interferencia en los datos y en el sistema, el abuso de los dispositivos, la falsificación y el fraude informático, la pornografía infantil y las infracciones de la propiedad intelectual y de los derechos afines. También tendrían cabida en este convenio ciertas disposiciones sobre derecho procesal, los principios generales que debían regir sobre la cooperación internacional, de suma importancia en este ámbito, y una serie de disposiciones finales.

Entre otras normativas destacadas, se debe señalar el Reglamento (CE) nº 460/2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información (ENISA), aprobado el 10 de marzo de 2004 y actualmente derogada. Por consiguiente, la ENISA es el organismo o agencia de la Unión Europea que aboga por que cada país alcance un estándar de ciberseguridad adecuado a las necesidades actuales. Entre otros, desempeña actividades dirigidas al desarrollo de las políticas de la Unión Europea en el ámbito cibernético, elabora esquemas de certificación de ciberseguridad para productos, servicios y procesos TIC y fomenta la cooperación entre los Estados miembros y los organismos de la Unión Europea, a la vez que les proporciona soporte a la hora de afrontar nuevas amenazas. Las competencias y funcionalidades de esta Agencia se vieron reforzadas por el Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, de manera que, con el paso del tiempo, se ha convertido en una autoridad supranacional en la materia.

En adición a lo anterior, en el año 2013 se desarrolla la Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro, en la que se aborda de una manera más específica el concepto de ciberespacio y se marcan las líneas de actuación necesarias para fomentar una cultura de ciberseguridad apropiada al paradigma actual. En este sentido, se marcan una serie de principios, como el acceso universal, seguro e íntegro a Internet y la necesidad de cooperación internacional, plasmados en una gobernanza multilateral democrática y eficaz y en la responsabilidad compartida. Además, establece una serie de prioridades y medidas estratégicas que se deben adoptar para solventar las problemáticas que circulan en torno al ciberespacio, que consisten en conseguir la ciberresiliencia, reducir de manera drástica la ciberdelincuencia, desarrollar estrategias y capacidades de ciberdefensa vinculadas a la Política Común de Seguridad y Defensa (PCSD), desarrollar recursos industriales y tecnológicos de ciberseguridad y establecer una política internacional coherente del ciberespacio para la Unión Europea, así como promover los valores esenciales de la Unión.

2.- Legislación en España

Dentro del ámbito nacional, en España el ciberespacio fue abordado por primera vez en legislación en el año 2008, dentro de la Directiva de Defensa Nacional, en el que era tratado como una nueva dimensión cuyas amenazas podrían interrumpir o condicionar el normal funcionamiento de la sociedad. En este sentido, el ciberespacio era abordado, si bien escuetamente, junto a amenazas tradicionalmente históricas como el terrorismo, el crimen organizado, la proliferación de armas de destrucción masiva, los Estados fallidos, débiles o en proceso de descomposición, los conflictos regionales, la lucha por el acceso a recursos básicos y el cambio climático. Además, otorgaba un papel a las Fuerzas Armadas y ciertas competencias para paliar los efectos que podía llegar a producir cada tipo de amenaza, al mismo tiempo que, en

el ámbito internacional, apoyaba el proceso de transformación de la OTAN, cuya finalidad era abordar los nuevos riesgos y amenazas.

A partir del año 2010, la ciberseguridad sería abordada desde una perspectiva integral que ya no emanaba exclusivamente de los organismos de defensa de la nación, sino que era fruto de una decisión interministerial. Esta circunstancia se pone de manifiesto con la entrada en vigor del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. En este punto, se abordan los principios básicos y requisitos mínimos exigibles para asegurar una protección adecuada de la información, que versan sobre la necesidad de que la seguridad sea entendida como un proceso integral, la gestión de la seguridad basada en los riesgos, los aspectos de prevención, reacción y recuperación, las líneas de defensa que deben adoptarse, la necesidad de una reevaluación periódica y la necesidad de diferenciación de las funciones en materia de seguridad. En adición a lo anterior, se regulan también en esta normativa las condiciones y requerimientos técnicos de las comunicaciones electrónicas, la aplicación de auditorías de seguridad y sus términos, y la forma de dar respuesta a los incidentes de seguridad, entre otros. En relación con esto último, se establece en esta normativa que el organismo encargado de articular la respuesta a los incidentes de seguridad será el CCN-CERT (Centro Criptológico Nacional-Computer Emergency Reaction Team), de manera que las Administraciones Públicas deben notificar al organismo aquellos incidentes que hubiesen producido un cierto impacto sobre la seguridad de la información y los servicios suministrados. Esta normativa fue actualizada con el Real Decreto 951/2015, de 23 de octubre, a consecuencia del rápido desarrollo que ha experimentado el ciberespacio, así como por la generalización de su uso y la constante evolución a la que han sido sometidas las nuevas amenazas, de manera que se ha profundizado en la materia e incluido nuevos preceptos que precisan la normativa.

Cabe mencionar, además, que el concepto de ciberespacio como nueva dimensión o escenario susceptible de contener amenazas, ha sido abordado en distintas normativas en España, como la Estrategia Española de Seguridad del año 2011, que lleva por título “Una responsabilidad de todos” y en la que comienza a contemplarse la posibilidad de aparición de actores pertenecientes a la criminalidad organizada o ciberterroristas, circunstancia que pone de relieve la necesidad de incrementar la seguridad de las infraestructuras críticas.

Dos años más tarde se publica la Estrategia Nacional de Seguridad, que lleva por título “Un proyecto compartido”, en la que se abordan, si bien desde una perspectiva generalista, las ciberamenazas y las líneas de acción estratégicas en ciberseguridad. Teniendo en cuenta lo anterior, en el año 2017 se actualiza la Estrategia Nacional de Seguridad, que pasa a denominarse “Un proyecto compartido de todos y para todos” y trata de profundizar en el concepto de ciberespacio y las amenazas intrínsecas a este nuevo ámbito, constituyendo los ciberataques y las ciberamenazas uno de los principales retos a la seguridad nacional actual.

El impulso de la ciberseguridad y la masiva utilización del ciberespacio, que ha permitido el traslado de actividades habitualmente concebidas para el espacio físico a poder ser realizadas dentro de un entorno virtual, han derivado, adicionalmente, en el desarrollo de un Código de Derecho de la Ciberseguridad, que fue aprobado en el año 2018 y actualizado por última vez el 23 de septiembre de 2020. Esta normativa realiza una recopilación de las principales leyes, tanto orgánicas como ordinarias, órdenes y Reales Decretos que se han dictado para regular las normativas de seguridad nacional, la protección de las infraestructuras críticas, la acción de los equipos de respuesta a incidentes de seguridad, el empleo de las telecomunicaciones por los usuarios, la ciberdelincuencia, la protección de datos y las relaciones con la administración.

Puedes encontrar la versión más reciente, en el momento de escribir estas líneas, en el siguiente enlace:

[file:///C:/Users/Amo%20Lean/Desktop/BOE-173 Codigo de Derecho de la Ciberseguridad.pdf](file:///C:/Users/Amo%20Lean/Desktop/BOE-173%20Codigo%20de%20Derecho%20de%20la%20Ciberseguridad.pdf)

Se trata de la actualización publicada en el Boletín Oficial del Estado en diciembre de 2020.

En relación con los organismos encargados de la respuesta a incidentes de seguridad, tal y como se ha mencionado anteriormente, en el ámbito nacional destaca el CCN-CERT, organismo concebido como la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN), que se encuentra adscrito al Centro Nacional de Inteligencia (CNI). El CCN-CERT constituye desde el año 2006 un CERT (Computer Emergency Response Team) Gubernamental Nacional dentro del ámbito español, cuyas competencias y alcance quedan reguladas por los Reales Decretos 421/2004, 3/2010 y 951/2015, de manera que, específicamente, se encomienda a este centro la gestión de todos los ciberincidentes que afecten a cualquier empresa u organismo público, si bien los casos más graves deben ser gestionados de manera conjunta por este servicio y el CNPIC, del que se hablará posteriormente. Así mismo, el CCN-CERT debe encargarse de coordinar las actividades que se desarrollan a nivel público de los Centros de Operaciones de Ciberseguridad (SOC) dedicados al desempeño de esta tarea.

No obstante, el CCN-CERT no es el único organismo encargado de estas funciones, destacando, entre otros, el Instituto Nacional de Ciberseguridad (INCIBE), que también tiene competencias en relación

con la respuesta a incidentes de seguridad, especialmente enfocadas al ciudadano y a los sectores empresariales estratégicos e infraestructuras críticas, llevando a cabo distintas iniciativas con las que se pretende incrementar los niveles de ciberseguridad existentes en España mediante mecanismos de colaboración público-privada. En adición a lo anterior, también se encarga de coordinar las actividades relacionadas con la ciberseguridad tanto a nivel nacional como internacional y de investigar las tendencias y posibilidad de riesgos emergentes, de manera que su enfoque no es solo reactivo, sino también preventivo, con la finalidad de elaborar mecanismos de alerta temprana que permitan solventar las amenazas en cuanto sea posible, siendo lo ideal antes de que lleguen a materializarse en algún tipo de impacto.

Por otro lado, el Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC) es el organismo encargado del desarrollo, coordinación y supervisión de todas las políticas y actividades que se lleven a cabo en relación con la ciberseguridad y la protección de las infraestructuras críticas en España, cuyo seno se encuentra en el Ministerio del Interior. Además, dentro del CNPIC se ubica la Oficina de Coordinación Cibernética (OCC), encargada de la coordinación técnica y la comunicación con los organismos INCIBE y CCN-CERT.

Por último, a nivel nacional cabe mencionar la labor del Mando Conjunto de Ciberdefensa (MCCD) o Mando Conjunto del Ciberespacio (MCCE), como ha pasado a denominarse en el año 2020, siendo este el organismo encargado de salvaguardar la libertad de acción de las Fuerzas Armadas en la dimensión del ciberespacio a través del planeamiento, dirección, coordinación, control y ejecución de las acciones conducentes a obtener tal efecto desde una perspectiva militar que se ajusta a los planes operativos en vigor. En adición a lo anterior, coopera con otros organismos de defensa como JEMAD, EMAD o EMACON con el objeto de garantizar la interoperabilidad de los sistemas, fomentar la transformación digital del Ministerio de Defensa

y sostener y desarrollar los medios para impulsar la ciberdefensa, entre otros.

En relación con los organismos que se encargan de combatir la cibercriminalidad dentro del ámbito español, cabe mencionar el cuerpo de la Guardia Civil y la Policía Nacional.

En relación con el cuerpo de la Guardia Civil, existe, en el seno de la Unidad Central Operativa, una sección denominada Grupo de Delitos Telemáticos (GDT), encargada de la investigación de todos los delitos que se perpetren a través de la red. Esta unidad, creada en el año 1996 bajo el nombre de Grupo de Delitos Informáticos (GDI), ha ido asumiendo competencias con el paso del tiempo y la proliferación de las nuevas ciberamenazas, de manera que en la actualidad se encarga tanto de la persecución de cualquier conducta delictiva que se produzca en el ciberespacio o atente contra los sistemas de información como de efectuar labores de concienciación que faciliten a los usuarios la utilización de las TIC de una forma segura. En este sentido, se han desarrollado en todas las provincias de España Equipos de Investigación Tecnológica (EDITE), que proporcionan al cuerpo la capacidad de responder al cibercrimen y asesorar a los ciudadanos de una manera más personalizada, incluso haciendo uso de las redes sociales más utilizadas por los usuarios para facilitar la comunicación con ellos.



- Miembros del Grupo de Trabajo para la Alianza Estratégica contra el Cibercrimen-

Por su parte, la Policía Nacional ha desarrollado en su seno una unidad denominada Brigada Central de Investigación Tecnológica (BCIT), a la que compete proporcionar una respuesta adecuada a las nuevas formas de ciberdelincuencia, tales como el fraude y las estafas cibernéticas, la pornografía infantil, los ciberataques, etcétera. Esta unidad, creada en el año 1995 y dependiente de la Unidad de Investigación Tecnológica (UIT), pertenece a la Dirección General de la Policía Judicial, de manera que se encarga de la investigación y obtención de pruebas relacionadas con la ciberdelincuencia, así como de perseguir a los actores que hayan llevado las acciones delictivas y ponerlos a disposición judicial. Al igual que ocurre con el cuerpo de la Guardia Civil, la Policía Nacional ofrece soporte a los usuarios a través de las redes sociales más utilizadas, habiendo trasladado y adaptado en buena parte su actividad, generalmente relacionada con el espacio físico, al entorno virtual.

En adición a lo anterior, existen otra serie de entidades que pueden operar tanto a nivel regional como nacional e incluso internacional y que ofrecen respuesta, apoyo y asesoramiento en relación con las amenazas, riesgos e incidentes de seguridad asociados al ciberespacio. Se trata de los CERT (Computer Emergency Response Team o, en castellano, Equipo de Respuesta ante Emergencias Informáticas), también denominados CSIRT (Computer Security Incident Response Team o, en castellano, Equipo de Respuesta a Incidentes de Seguridad Informática), que, pudiendo proceder tanto del sector público como del sector privado, se ocupan de proporcionar una respuesta adecuada a las amenazas a la ciberseguridad, generalmente tanto de tipo preventivo como reactivo, si bien sus funciones en concreto quedan reguladas por las normativas de cada país.

En relación con las acciones de tipo preventivo que suelen llevar a cabo esta clase de equipos puede hablarse de la emisión de boletines y avisos informativos relacionados con la ciberseguridad, de distinta índole, la realización de auditorías de seguridad y la búsqueda de sistemas vulnerables, así como la elaboración de un bastionado correcto de los sistemas de cada entidad, entre otros. Por otro lado, en relación con las acciones de tipo reactivo, cada CERT o CSIRT, por lo general, tiene competencias en materia de gestión de incidentes que afectan a la seguridad informática. Cabe señalar que, si bien los términos CERT y CSIRT se usan indistintamente para describir a los Equipos de Respuesta ante Incidentes de Seguridad, la primera denominación tiende a utilizarse en mayor medida en Estados Unidos, constituyendo además un término registrado por Carnegie Mellon University y debiendo ser autorizada cada entidad en concreto por esta organización para certificarse de manera pública como CERT, mientras que CSIRT es la denominación más utilizada en Europa.

Actualmente, según expone ENISA, existen 54 equipos que adquieren la denominación de CERT o CSIRT en España. En los párrafos anteriores ya se ha hablado de algunos organismos públicos a nivel estatal que cuentan con la capacitación de CERT o CSIRT, tales

como el CCN-CERT o el INCIBE-CERT, mientras que a nivel regional también están catalogados de esta forma organismos como AndalucíaCERT, BCSC o CATALONIAN-CERT, entre otros. En el ámbito privado existen, entre otras organizaciones, los equipos ENTELGY-CSIRT o Santander Global CERT. A nivel internacional opera, por ejemplo, el CERT-EU, creado por el conjunto de instituciones de la Unión Europea el 11 de septiembre del año 2012, que se congregaron para desarrollar un equipo que proporcionase soporte a todos los países de la Unión y con el objeto de promover el desarrollo de una red europea de equipos de respuesta ante incidentes que afecten a la ciberseguridad.

Con la finalidad de proporcionar una respuesta adecuada y eficaz a las ciberamenazas, se ha creado lo que se conoce como Centros de Operaciones de Seguridad (SOC - Security Operations Center), esto es, espacios en los que distintos equipos especializados trabajan en la búsqueda, investigación, seguimiento y análisis de toda actividad anómala que pudiese tener lugar en los sistemas y pudiese ser indicativa de la existencia de un incidente de seguridad informático, así como de prevenir el posible compromiso de los sistemas o de la información mediante el desarrollo y fomento de buenas prácticas de ciberseguridad.

Por lo general, entre los servicios con los que cuenta un SOC suelen encontrarse servicios de monitorización de riesgos y amenazas, servicios de gestión de incidentes de seguridad, servicios de análisis forense y servicios de inteligencia de amenazas, entre otros. Además, cabe mencionar lo que se conoce como Red Team, Blue Team y Purple Team. El Red Team es un equipo de profesionales que realiza labores de seguridad ofensiva, es decir, que simula constituir un equipo de ciberatacantes, utilizando sus mismas técnicas y herramientas u otras similares para construir escenarios de posibles amenazas que permitan definir las necesidades de seguridad y protección de cada organización, así como conocer su capacidad real de detección y respuesta ante posibles ciberataques. El Blue Team, por el contrario, lo constituye un equipo de profesionales que realiza actividades de seguridad defensiva,

esto es, que efectúa labores permanentes de vigilancia proactiva y monitorización, tratando de identificar posibles comportamientos anómalos en los sistemas y las redes y brindando la posibilidad de implementar planes de actuación que permitan mitigar o disminuir los riesgos existentes. Por último, el Purple Team lo constituye un equipo de profesionales que trata de aunar las técnicas y actividades desempeñadas por los dos equipos anteriores con la finalidad de incrementar la eficacia de cada equipo, es decir, trata de poner a prueba la seguridad de los activos de cada organización al mismo tiempo que realiza una monitorización coordinada de los archivos de registro y evalúa las capacidades de detección de la organización.

Para terminar con los organismos y formas de luchar contra las amenazas a la seguridad informática, a nivel internacional, además de ENISA, se debe hacer referencia a varios organismos que operan para fomentar una cultura de ciberseguridad y ciberdefensa a la par que combaten el cibercrimen.

En primer lugar, cabe señalar la Organización Internacional de Policía Criminal (INTERPOL), de la que hasta 194 países forman parte actualmente. Este organismo, que, de manera genérica, se encarga de procurar la colaboración, cooperación y el intercambio de información sobre actividades delictivas y delincuentes con los cuerpos policiales de cada país, además de proporcionarles asistencia técnica y operativa en el desarrollo de sus funciones, también se ocupa de la investigación y la lucha contra las ciberamenazas a nivel internacional, estableciendo mecanismos de colaboración, coordinando una respuesta global y fomentando la capacitación y formación para desarrollar habilidades cibernéticas que permitan abordar la ciberdelincuencia de forma efectiva.

Por otro lado, a nivel europeo se debe citar Europol, el organismo encargado de proporcionar soporte a todos los estados miembros de la Unión Europea en relación con la lucha contra la delincuencia internacional y el terrorismo. Dentro de Europol se han desarrollado dos

organizaciones especialmente dedicadas al combate de la ciberdelincuencia:

- European Union Cybercrime Task Force (EUCTF), que, desde su creación en el año 2010, constituye una red de confianza de la que forman parte los responsables de las unidades nacionales de ciberdelincuencia de todos los países de la Unión Europea y sus países asociados (Dinamarca, Islandia, Noruega y Suiza), a los que reúne dos veces cada año junto a otros organismos oficiales para identificar, debatir y priorizar los desafíos y acciones clave en la lucha contra la ciberdelincuencia.

- European Cybercrime Centre (EC3), que, desde su creación en el año 2013, se encarga de asistir a los países de la Unión Europea en la lucha contra el ciberdelito, fortaleciendo la respuesta policial de cada país y proporcionando asistencia técnica y operativa sobre operaciones de alto perfil, a la vez que elabora, anualmente, un informe estratégico denominado Internet Organised Crime Threat Assessment (IOCTA), el cual trata de evaluar posibles amenazas emergentes relacionadas con el cibercrimen

CAPÍTULO IV: BIBLIOGRAFÍA

A continuación, tenéis las fuentes utilizadas para elaborar las páginas anteriores; todas ellas están disponible on-line para aquellos que quieran ampliar su conocimiento sobre asuntos concretos entre los mencionados en las páginas anteriores:

- Abraham, S. (2018). Lista de Tipos de Malware. *MalwareFox*. Recuperado de <https://www.malwarefox.com/es/lista-de-tipos-de-malware/>.

- Albors, J. (2015). Ataque a Ashley Madison comprometería a 37 millones en citas extramatrimoniales. ESET. Recuperado de <https://www.welivesecurity.com/la-es/2015/07/20/ataque-ashley-madison/>.

- Albors, J. (2014). ¿Sabes qué es un exploit y cómo funciona? *ESET*. Recuperado de <https://www.welivesecurity.com/la-es/2014/10/09/exploits-que-son-como-funcionan/>.

- Álvarez, R. (2017). El hackeo a Yahoo fue más grave de lo que pensábamos: 3.000 millones de cuentas robadas (todas las que tenía en 2013). Xataka. Recuperado de <https://www.xataka.com/seguridad/el-hackeo-a-yahoo-fue-mas-grave-de-lo-que-pensabamos-3-000-millones-de-cuentas-robadas-todas-las-que-tenia-en-2013>.

- Álvarez, R. (2016). ¿Han hackeado a la NSA? Esto es todo lo que se sabe hasta el momento. Xataka. Recuperado de <https://www.xataka.com/seguridad/han-hackeado-a-la-nsa-esto-es-todo-lo-que-se-sabe-hasta-el-momento>.

- Antolínez, S. (2001). Code Red. Computer World. Recuperado de <https://www.computerworld.es/economia-digital/code-red>.

- Araújo, S. (2018). Qué es la Deep Web y en qué se diferencia de la Dark Web. Genbeta. Recuperado de <https://www.genbeta.com/a-fondo/que-es-la-deep-web-y-en-que-se-diferencia-de-la-dark-web>.

- Ayuso, M. (2018). El primer ciberataque tuvo lugar hace 200 años (y ofrece valiosas lecciones hoy). La Información. Recuperado de <https://www.lainformacion.com/management/el-primer-ciberataque-tuvo-lugar-hace-200-anos-y-ofrece-valiosas-lecciones-hoy/6349379>.

- Ballota, D. (2012). Por tierra, mar, aire, espacio y ciberespacio. Genbeta. Recuperado de <https://www.genbeta.com/activismo-online/por-tierra-mar-aire-espacio-y-ciberespacio>.

- Barbieri, A. (2019). La historia del hacker que detuvo al virus WannaCry y terminó encarcelado. La Vanguardia. Recuperado de <https://www.lavanguardia.com/tecnologia/20190502/461931480386/h-eroe-villano-informatico-hacker-wannacry-hutchins-mcafee-jonathan-james-lazarus.html>.

- Barroso, D. (2016). El replanteamiento de la ciberseguridad. Slideshare. Recuperado de <https://www.slideshare.net/lostinsecurity/el-replanteamiento-de-la-ciberseguridad>.

- BBC Mundo (2016). Caso "Celebgate": aparece otro culpable del pirateo de fotografías íntimas de Jennifer Lawrence y otras famosas de Hollywood. BBC News. Recuperado de <https://www.bbc.com/mundo/noticias-36691109>.

- Bejerano, P. (2014). Código Enigma, descifrado: el papel de Turing en la Segunda Guerra Mundial. *El Diario*. Recuperado de https://www.eldiario.es/turing/criptografia/alan-turing-enigma-codigo_0_226078042.html.

- Bergel, G. (2019). Lazarus, levántate y camina... Blog Think Big. Recuperado de <https://empresas.blogthinkbig.com/analisis-grupo-lazarus-ciberseguridad/>.

- Cantón, D. (2015). Clasificación de ataques DoS. *Certsi*. Recuperado de <https://www.certsi.es/blog/clasificacion-ataques-dos>.

- Calles, J. A. (2018). #TTPs y la Pirámide del Dolor. *Flu-Project*. Recuperado de <https://www.flu-project.com/2018/04/ttps-y-la-piramide-del-dolor.html>.

- Condliffe, J. (2016). La historia completa de los ciberataques masivos e interminables a Yahoo. MIT Technology Review. Recuperado de <https://www.technologyreview.es/s/6582/la-historia-completa-de-los-ciberataques-masivos-e-interminables-yahoo>.

- Crisol, L. (2016). Una organización hacker de la NSA parece haber sido hackeada. *Computer Hoy*. Recuperado de <https://computerhoy.com/noticias/software/organizacion-hacker-nsa-parece-haber-sido-hackeada-49628>.

- Fernández, Y. (2017). La historia de Creeper, el primer virus informático jamás programado. *Xataka*. Recuperado de <https://www.xataka.com/historia-tecnologica/la-historia-de-creeper-el-primero-virus-informatico-jamas-programado>.

- García, A. (2017). WannaCry 2.0: el ransomware Petya ataca a nuevas empresas de España y Europa. ADSL Zone. Recuperado de <https://www.adslzone.net/2017/06/27/wannacry-2-0-el-ransomware-petya-ataca-nuevas-empresas-de-espana-y-europa/>.

- Garzón, T. (2017). El ciberactivismo en las revoluciones posmodernas. *Revista de Estudios en Seguridad Internacional*. Recuperado de <http://www.seguridadinternacional.es/revista/?q=content/el-ciberactivismo-en-las-revoluciones-posmodernas>.

- González, M. (2014). Si hay un ciberataque que merece ser llamado "de película", ése es el sufrido por Sony Pictures. Xataka. Recuperado de <https://www.xataka.com/aplicaciones/si-hay-un-ciberataque-que-merece-ser-llamado-de-pelicula-ese-es-el-sufrido-por-sony-pictures>.

- GReAT (2013). "Red October" Diplomatic Cyber Attacks Investigation. Kaspersky. Recuperado de <https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/>.

- Huete, C. (2019). ¿Cuáles son los principales organismos relacionados con la ciberseguridad? IMF Business School. Recuperado de <https://blogs.imf-formacion.com/blog/tecnologia/organismos-ciberseguridad-201904/>.

- INCIBE (2018). Threat Intelligence: Desde qué es hasta cómo lo hago (W. Nykiel) T7 - CyberCamp 2017. *Youtube*. Recuperado de https://www.youtube.com/watch?v=Xk75Fa_YZfQ.

- INCIBE (2017). Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian? *Instituto Nacional de Ciberseguridad*. Recuperado de <https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian>.

- Jaimovich, D. (2018). Cómo surgió y se propagó WannaCry, uno de los ciberataques más grandes de la historia. Infobae. Recuperado de <https://www.infobae.com/america/tecno/2018/05/12/como-surgio-y-se-propago-wannacry-uno-de-los-ciberataques-mas-grandes-de-la-historia/>.

- Jiménez Domínguez, D. Privacidad de la información. Ataques dirigidos. *Universidad Nacional Autónoma de México*. Recuperado de <https://revista.seguridad.unam.mx/numero-05/privacidad-de-la-informaci%C3%B3n-ataques-dirigidos>.

- Julián, G. (2013). Stuxnet: historia del primer arma de la ciberguerra. Genbeta. Recuperado de <https://www.genbeta.com/seguridad/stuxnet-historia-del-primer-arma-de-la-ciberguerra>.

- Kubovič, O. (2019). Detecciones de EternalBlue alcanzan nuevo pico desde el brote de WannaCryptor. ESET. Recuperado de <https://www.welivesecurity.com/la-es/2019/05/17/detecciones-eternalblue-alcanza-nuevo-pico-desde-wannacry/>.

- Latto, N. (2020). ¿Qué es WannaCry? Avast. Recuperado de <https://www.avast.com/es-es/c-wannacry>.

- León, D. (2018). TTPs y la Pirámide del Dolor. Zerolynx. Recuperado de <https://blog.zerolynx.com/2018/04/ttps-y-la-piramide-del-dolor.html>.

- Lipovsky, R. (2017). A siete años de Stuxnet, los sistemas industriales están nuevamente en la mira. We Live Security. Recuperado de <https://www.welivesecurity.com/la-es/2017/06/20/sistemas-industriales-en-la-mira/>.

- López, D. Evolución de la Seguridad Informática. *Empresa de Seguridad Grupo Control S.A.* Recuperado de <https://www.grupocontrol.com/evolucion-de-la-seguridad-informatica>.

- Marín, E. (2014). El ataque a Sony Pictures es el mayor «hacking» que ha sufrido la industria del cine. Hipertextual. Recuperado de <https://hipertextual.com/2014/12/sony-pictures-hackers>.

- Martí, A. (2017). The Shadow Brokers: su historia desde el hacking a la NSA hasta la venta de "exploits" por suscripción mensual. Xataka. Recuperado de <https://www.xataka.com/seguridad/the-shadow-brokers-su-historia-desde-el-hacking-a-la-nsa-hasta-la-venta-de-exploits-por-suscripcion-mensual>.

- Martín, A. (2015). Hacking Team, el sistema de vigilancia de muchos países, ha sido hackeado. Hipertextual. Recuperado de <https://hipertextual.com/2015/07/hacking-team-hackeado>.

- Merino, M. (2020). Kilos se convierte en el sucesor de Grams como 'Google de la Dark Web'. Genbeta. Recuperado de <https://www.genbeta.com/actualidad/kilos-se-convierte-sucesor-grams-como-google-dark-web>.

- Migoya Edualden, J. M. (2020). Curso de Analista SOC. Módulo de Respuesta ante Incidentes. Escuela de Organización Industrial.

- Migoya Edualden, J. M. (2013). Visión actual de la seguridad. *InnoTec System. Entelgy*.

- Mora, A. (2018). ¿Qué es la dark web? ¿Qué es la deep web? Te lo explicamos. *PCWorld*. Recuperado de <https://www.pcworld.es/articulos/internet/dark-web-deep-web-3673874/>.

- Motos, V. (2016). "Purple teams": combinando ataque y defensa. Hack Players. Recuperado de <https://www.hackplayers.com/2016/04/purple-teams-combinando-ataque-y-defensa.html>.

- Nava Garcés, A. E. (2017). Ciberterrorismo: La nueva cara de la delincuencia en el siglo XXI. Foro Jurídico. Recuperado de <https://www.forojuridico.org.mx/ciberterrorismo/>.

- Ng, A. (2017). Yahoo: Masivo ciberataque afectó a todas sus 3,000 millones de cuentas. CNet. Recuperado de <https://www.cnet.com/es/noticias/yahoo-masivo-ciberataque-afecto-a-3000-millones-de-cuentas/>.

- Paganini, P. (2015). CyberCriminals and their APT and AVT Techniques. Security Affairs. Recuperado de <https://securityaffairs.co/wordpress/33999/cyber-crime/apt-and-avt-techniques.html>.

- Patricio Sánchez, E. (2016). Inteligencia de amenazas ¿Cómo entenderla? *Magazciturum*. Recuperado de <http://www.magazciturum.com.mx/?p=3415#.W1XAa9L7TIV>.

- Pascual Estapé, J. A. (2014). Grams, buscador de droga, armas y otros productos prohibidos. Computer Hoy. Recuperado de <https://computerhoy.com/noticias/internet/grams-buscador-droga-armas-otros-productos-prohibidos-11911>.

- Pastor, J. (2018). WannaCry, un año después. Xataka. Recuperado de <https://www.xataka.com/seguridad/wannacry-un-ano-despues>.

- Pastor, J. (2017). NotPetya: así actúa el nuevo ransomware que está causando el caos, y así puedes detener su avance. Xataka. Recuperado de <https://www.xataka.com/seguridad/notpetya-asi-actua>

[el-nuevo-ransomware-que-esta-causando-el-caos-y-asi-puedes-detener-su-avance.](#)

- Pérez Fernández, D. (2018). El Exploit "DoublePulsar" de la NSA ahora funciona en sistemas Windows IoT. Recuperado de <https://tecnonucleous.com/2018/06/28/exploit-doublepulsar-funciona-en-windows-iot/>.

- Pintado, C. (2014). Stuxnet, la primera batalla de la guerra de Irán. CISDE. Recuperado de <https://observatorio.cisde.es/archivo/stuxnet-la-primera-batalla-de-la-guerra-de-iran/>.

- Rotten, J. A. (2018). Siglo XVIII: El primer ciberataque de la historia. *Blog Intrínseco y expectorante*. Recuperado de <http://intrinsecoyespectorante.blogspot.com/2018/05/siglo-xviii-el-primer-ciberataque-de-la.html>.

- Ruiz, D. (2015). Los hackers atacan 'Hacking Team', una empresa que vende programas espía a gobiernos. La Vanguardia. Recuperado de <https://www.lavanguardia.com/internacional/20150706/54433232001/hacking-team-gigas-informacion-confidencial.html>.

- Sánchez Silva, D. (2017). The Shadow Brokers – Seguimiento de las acciones de TSB. Tarlogic. Recuperado de <https://www.tarlogic.com/blog/the-shadow-brokers/>.

- Sin autor (2020). Código de Derecho de la Ciberseguridad. Boletín Oficial del Estado. Recuperado de https://www.boe.es/biblioteca_juridica/codigos/codigo.php?id=173_Codigo_de_Derecho_de_la_Ciberseguridad&modo=2.

- Sin autor (2020). Historia de los virus informáticos. Tecnología + Informática. Recuperado de <https://www.tecnologia-informatica.com/historia-virus-informaticos/>.

- Sin autor (2020). Los tipos de ciberataques a empresas más frecuentes. Viewnext. Recuperado de <https://www.viewnext.com/tipos-de-ciberataques-a-empresas/>.

- Sin autor (2020). Red Team, Blue Team y Purple Team, ¿cuáles son sus funciones y diferencias? UNIR. Recuperado de <https://www.unir.net/ingenieria/revista/red-blue-purple-team-ciberseguridad/>.

- Sin autor (2019). Dark Web: riesgos, contenidos y cómo acceder [Guía Práctica]. LISA Institute. Recuperado de <https://www.lisainstitute.com/blogs/blog/dark-web-riesgos-contenidos-como-acceder>.

- Sin autor (2019). ¿Qué es un SOC y qué actividades realiza? IMF Business School. Recuperado de <https://blogs.imf-formacion.com/blog/tecnologia/que-es-soc-actividades-realiza-201903/>.

- Sin autor (2019). Qué es un Centro de Operaciones de Ciberseguridad (SOC) y para qué sirve. EALDE Business School. Recuperado de <https://www.ealde.es/que-es-centro-operaciones-ciberseguridad/>.

- Sin autor (2019). Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo. EUR-Lex. Recuperado de <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32019R0881&from=EN>.

- Sin autor (2018). Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad. *Blog especializado en Sistemas de Gestión de Seguridad de la Información*. Recuperado de <https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/>.

- Sin autor (2018). Toda la verdad detrás del escandaloso robo y difusión de fotografías de famosas desnudas. ABC. Recuperado de https://www.abc.es/estilo/gente/abci-celebgate-toda-verdad-detras-escandaloso-robo-y-difusion-fotografias-famosas-desnudas-201811231357_noticia.html#ancla_comentarios.

- Sin autor (2017). De Wannacry a Petya: cómo un 'ransomware' ha paralizado (otra vez) el mundo. El Confidencial. Recuperado de https://www.elconfidencial.com/tecnologia/2017-06-28/petya-ransomware-ciberataque-wannacry_1406044/.

- Sin autor (2017). Estrategia de Seguridad Nacional. La Moncloa. Recuperado de https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/presidencia/gobierno/Documents/2017-1824_Estrategia_de_Seguridad_Nacional_ESN_doble_pag.pdf.

- Sin autor (2017). Petya, nuevo ataque mundial de ransomware. INCIBE-CERT. Recuperado de <https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/petya-nuevo-ataque-mundial-ransomware>.

- Sin autor (2017). Una nueva ola de ciberataques que empezó en Ucrania se extiende por el mundo. La Vanguardia. Recuperado de <https://www.lavanguardia.com/internacional/20170627/423728612720/ciberataque-ransonware-wannacry.html>.

- Sin autor (2016). 5 cosas que debes saber sobre la Ingeniería Social. *ESET*. Recuperado de <https://www.welivesecurity.com/la-es/2016/01/06/5-cosas-sobre-ingenieria-social/>.

- Sin autor (2016). Introducción a la ciberseguridad (I): Qué es y por qué importa. *El Blog de Indea*. Recuperado de <http://indeadiversity.com/ciberseguridad-que-es-por-que-importa/>.

- Sin autor (2016). Martes de retrospectiva: el gusano Morris. *We Live Security*. Recuperado de <https://www.welivesecurity.com/la-es/2016/11/08/retrospectiva-gusano-morris/>.

- Sin autor (2015). Ataque dirigido, ¿qué es y porqué es tan peligroso? *Tecno XXI*. Recuperado de <https://www.tecnoxxi.com/blog/seguridad/ataque-dirigido-que-es-y-por-que-es-tan-peligroso/>.

- Sin autor (2015). El virus que tomó control de mil máquinas y les ordenó autodestruirse. *BBC News*. Recuperado de https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet.

- Sin autor (2015). Filtran 400GB de información confidencial del grupo Hacking Team. *ESET*. Recuperado de <https://www.welivesecurity.com/la-es/2015/07/06/filtran-400gb-de-informacion-confidencial-del-grupo-hacking-team/>.

- Sin autor (2015). Hackean la empresa de espionaje italiana Hacking Team, que sirve a gobiernos de todo el mundo. *RTVE*. Recuperado de <https://www.rtve.es/noticias/20150707/hackean-empresa-espionaje-italiana-hacking-team-sirve-gobiernos-todo-mundo/1174563.shtml>.

- Sin autor (2015). Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Boletín Oficial del Estado. Recuperado de <https://www.boe.es/buscar/doc.php?id=BOE-A-2015-11881>.

- Sin autor (2014). Aprendiendo a identificar los 10 phishing más utilizados por ciberdelincuentes. *Oficina de Seguridad del Internauta*. Recuperado de <https://www.osi.es/es/actualidad/blog/2014/04/11/aprendiendo-identificar-los-10-phishing-mas-utilizados-por-ciberdelincuen>.

- Sin autor (2014). El ciberataque a Sony, un drama de graves consecuencias para Hollywood. La Vanguardia. Recuperado de <https://www.lavanguardia.com/cultura/20141216/54421480922/el-ciberataque-a-sony-un-drama-de-improbable-final-feliz.html>.

- Sin autor (2014). Guardians of Peace sigue con su extorsión a Sony y filtrando datos de famosos. La Vanguardia. Recuperado de <https://www.lavanguardia.com/gente/20141210/54421263777/guardians-of-peace-extorsion-sony-filtrando-datos-famosos.html>.

- Sin autor (2014). «Wiper», el «gusano» utilizado en el ciberataque a Sony Pictures. ABC. Recuperado de <https://www.abc.es/tecnologia/redes/20141225/abci-wiper-virus-ataque-sony-201412241549.html>.

- Sin autor (2013). Comunicación conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro. EUR-Lex. Recuperado de <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52013JC0001>.

- Sin autor (2013). Estrategia de Seguridad Nacional 2013. Departamento de Seguridad Nacional. Recuperado de <https://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-seguridad-nacional>.

- Sin autor (2013). Octubre Rojo. El malware más “diplomático”. INCIBE. Recuperado de <https://www.incibe-cert.es/blog/octubre-rojo>.

- Sin autor (2013). ¿Qué es una APT? *Kaspersky Lab*. Recuperado de <https://www.kaspersky.es/blog/que-es-una-apt/966/>.

- Sin autor (2011). Ciberactivismo y Ciberguerra, a debate en el III Security Blogger Summit. Panda Security. Recuperado de <https://www.pandasecurity.com/spain/mediacenter/notas-de-prensa/ciberactivismo-y-ciberguerra-a-debate-en-el-iii-security-blogger-summit/>.

- Sin autor (2011). Estrategia Española de Seguridad. Una responsabilidad de todos. Gobierno de España. Real Instituto Elcano. Recuperado de <http://www.realinstitutoelcano.org/wps/wcm/connect/c06cac0047612e998806cb6dc6329423/EstrategiaEspanolaDeSeguridad.pdf?MOD=AJPERES&CACHEID=c06cac0047612e998806cb6dc6329423>.

- Sin autor (2010). Instrumento de Ratificación del Convenio sobre la Ciberdelincuencia, hecho en Budapest el 23 de noviembre de 2001. Boletín Oficial del Estado. Recuperado de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221.

- Sin autor (2010). Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Boletín Oficial del Estado. Recuperado de <https://www.boe.es/buscar/act.php?id=BOE-A-2010-1330>.

- Sin autor (2008). Directiva de Defensa Nacional 01/2008. Consejo de Defensa Nacional. Recuperado de <https://armada.defensa.gob.es/ArmadaPortal/ShowProperty?nodePath=/BEA%20Repository/Desktops/Portal/ArmadaEspañola/Pages/mardigitaldocinstituc/01docu-institucional-defensa/05directiva-defensa-nacional/01directivadefensanacional-es/doc01directivadefensanacional08//archivo>.

- Sin autor (2004). Reglamento (CE) nº 460/2004 del Parlamento Europeo y del Consejo, de 10 de marzo de 2004, por el que se crea la Agencia Europea de Seguridad de las Redes y de la Información (Disposición derogada). CIDO. Recuperado de <http://cido.diba.cat/legislacio/465776/reglamento-ce-n-4602004-del-parlamento-europeo-y-del-consejo-de-10-de-marzo-de-2004-por-el-que-se-crea-la-agencia-europea-de-seguridad-de-las-redes-y-de-la-informacion>.

- Sin autor (2001). El genio del virus que paralizó el mundo. El Mundo. Recuperado de <https://www.elmundo.es/navegante/2001/02/06/entrevistas/981454491.html>.

- Sin autor. About ENISA - The European Union Agency for Cybersecurity. European Union Agency for Cybersecurity. Recuperado de <https://www.enisa.europa.eu/about-enisa>.

- Sin autor. About us. CERT-EU. Recuperado de https://cert.europa.eu/cert/plainedition/en/cert_about.html.

- Sin autor. Acerca de Europol. EUROPOL. Recuperado de <https://www.europol.europa.eu/es/about-europol>.

- Sin autor. B.C.I.T. - ¿Quiénes somos? Dirección General de la Policía. Recuperado de https://www.policia.es/org_central/judicial/udef/bit_quienes_somos.html.

- Sin autor. CERT/CSIRT. Secur-IT @C.R.S. Recuperado de <https://securit.blog/knowledge-base/certcsirt/>.

- Sin autor. Cibercriminalidad. Ministerio del Interior. Recuperado de <http://www.interior.gob.es/documents/10180/1207668/Avance+datos+cibercriminalidad+2013.pdf/5de24ec6-b1cc-4451-bd06-50d93c006815>.

- Sin autor. Ciberespacio. EcuRed. Recuperado de <https://www.ecured.cu/Ciberespacio>.

- Sin autor. CNPIC. CSIRT.es. Recuperado de <https://www.csirt.es/index.php/es/miembros/cnpic>.

- Sin autor. Cronología de los ciberataques. *Revista de la OTAN*. Recuperado de <https://www.nato.int/docu/review/2013/Cyber/timeline/ES/index.htm>.

- Sin autor. CSIRTs by Country - Interactive Map. European Union Agency for Cybersecurity. Recuperado de <https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map#country=Spain>.

- Sin autor. ¿Cuáles son los ciberataques más comunes? Cisco. Recuperado de https://www.cisco.com/c/es_mx/products/security/common-cyberattacks.html.

- Sin autor. Cyber capabilities development. INTERPOL. Recuperado de <https://www.interpol.int/Crimes/Cybercrime/Cyber-capabilities-development>.

- Sin autor. Cybercrime. INTEPROL. Recuperado de <https://www.interpol.int/Crimes/Cybercrime>.

- Sin autor. ENS: Dimensiones de la Seguridad. CCN-CERT. Recuperado de <https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1067>.

- Sin autor. EUCTF. EUROPOL. Recuperado de <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf>.

- Sin autor. European Cybercrime Centre – EC3. EUROPOL. Recuperado de <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>.

- Sin autor. Hidden Wiki .onion Urls Tor Link Directory. Hidden Wiki. Recuperado de <https://thehiddenwiki.org/>.

- Sin autor. La unidad. Grupo de Delitos Telemáticos. Unidad Central Operativa. Recuperado de https://www.gdt.guardiacivil.es/webgdt/la_unidad.php.

- Sin autor. Mando Conjunto de Ciberespacio. Ministerio de Defensa. Recuperado de <https://emad.defensa.gob.es/unidades/mcce/>.

- Sin autor. Misión y objetivos. CCN-CERT. Recuperado de <https://www.ccn-cert.cni.es/sobre-nosotros/mision-y-objetivos.html>.

- Sin autor. Otras Preguntas: 1034 - ¿Qué significa No Repudio o Irrenunciabilidad? Fábrica Nacional de Moneda y Timbre. Recuperado de <https://www.sede.fnmt.gob.es/preguntas-frecuentes/otras-preguntas/>

[/asset_publisher/1RphW9IeUoAH/content/1034-que-significa-no-repudio-o-irrenunciabilidad-](#).

- Sin autor. Política de Seguridad. Open Data Security. Recuperado de <https://opendatasecurity.io/es/politica-de-seguridad/>.

- Sin autor. ¿Por qué internet y el ciberespacio no son lo mismo? Linube. Recuperado de <https://linube.com/blog/ciberespacio-no-es-internet/>.

- Sin autor. ¿Qué es el ransomware WannaCry? Kaspersky. Recuperado de <https://www.kaspersky.es/resource-center/threats/ransomware-wannacry>.

- Sin autor. ¿Qué es INTERPOL? INTERPOL. Recuperado de <https://www.interpol.int/es/Quienes-somos/Que-es-INTERPOL>.

- Sin autor. ¿Qué es la ciberseguridad? Kaspersky Lab. Recuperado de <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>.

- Sin autor. Qué hacemos. Instituto Nacional de Ciberseguridad. Recuperado de <https://www.incibe.es/que-es-incibe/que-hacemos>.

- Sin autor. Safety 101: Los tipos de malware. Kaspersky Lab. Recuperado de <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>.

- Sin autor. Seguridad de la información. Universidad de Oviedo. Recuperado de <http://isa.uniovi.es/docencia/SIGC/pdf/certificados.pdf>.

- Sin autor. Sistema de Gestión de Seguridad de la Información. Red.es. Recuperado de <https://www.red.es/redes/es/node/7750>.

- Sin autor. The CERT Division. Carnegie Mellon University. Recuperado de <https://www.sei.cmu.edu/about/divisions/cert/>.

- Sin autor. Una breve historia de los virus informáticos y lo que nos deparará el futuro. Kaspersky. Recuperado de <https://latam.kaspersky.com/resource-center/threats/a-brief-history-of-computer-viruses-and-what-the-future-holds>.

- Thomas, K. (2015). Caso Ashley Madison: la cronología de los hechos. ESET. Recuperado de <https://www.welivesecurity.com/la-es/2015/08/31/caso-ashley-madison-cronologia/>.

- Varma, S. (2017). Petya ransomware targeted Ukraine but India also affected badly, experts call it wiper. India Today. Recuperado de <https://www.indiatoday.in/technology/features/story/petya-ransomware-india-worst-affected-in-asia-everything-to-know-about-this-wiper-985354-2017-06-29>.

- Yúbal FM (2018). ¿Cuál es la diferencia: malware, virus, gusanos, spyware, troyanos, ransomware, etcétera? *Xataka*. Recuperado de <https://www.xataka.com/basics/cual-es-la-diferencia-malware-virus-gusanos-spyware-troyanos-ransomware-etcetera>.

- Yúbal FM (2018). Deep Web, Dark Web y Darknet: éstas son las diferencias. *Xataka*. Recuperado de <https://www.xataka.com/aplicaciones/deep-web-dark-web-y-darknet-cuales-son-las-diferencias>.

PARTE II:

AYUDAS DE JUEGO

CAPÍTULO V: CONSEJOS PARA USAR CIBERSEGURIDAD EN KARMA

1.- Antes que nada: que no cunda el pánico

Ese es, sin duda, el primer consejo que, Director de Juego o personaje jugador, se te debe transmitir: no te asustes, no te bloques, no pienses que esta avalancha de información te supera, no dejes que tus conexiones neuronales se saturen, sufriendo una suerte de síndrome de Stendhal rolero. No te sientas desbordado.

Recuerda: esto es una ayuda de juego.

Eso significa que solo está para ayudarte a mejorar tus partidas, tu experiencia en la mesa de juego.

La ciberseguridad, por su naturaleza técnica, es un campo complejo. ¿Cuándo lees sobre ello tu cabeza amenaza con explotar? Tranquila, o tranquilo. Te contaremos un secreto: a nosotros también. Raquel Puebla ha hecho un trabajo extraordinario en la primera parte del suplemento enseñándonos a todos una serie de ideas básicas sobre seguridad y sobre su historia, y nosotros, a continuación, queremos ofrecerte una serie de recomendaciones e informaciones sobre cómo introducir esas temáticas y conocimientos en tus partidas de rol. Pero la idea no es que tomes todo lo que has leído ya y lo que leerás en las páginas siguientes, sino que busques solo aquellas cosas que beneficien

tu experiencia. Puede ser tanto como para construir una aventura entera en el ciberespacio o tan poco como unos cuantos términos técnicos que poner en boca de un PNJ con el que se crucen tus personajes en una aventura que nada tiene que ver con la ciberseguridad. Con que este módulo simplemente para introducir un término técnico en boca de un informático que toma café en el mismo local que los protagonistas de tu aventura, el suplemento habrá cumplido su función.

Ese es el consejo clave para abordar el módulo: picotea aquello que te interesa, entresaca lo que pueda ayudarte en tu mesa de juego.

Puedes -¿puedes? ¡¡Debes!!- prescindir de todo aquello que no te sirva para eso. Cualquier información, cualquier dato, cualquier regla, cualquier sugerencia que amenace con introducir un elemento de incomodidad a tu partida, bórralo de inmediato.

¿Qué significa eso? Quédate solo con lo que te ayude.

Todo lo que te parezca demasiado complejo, demasiado enrevesado, que complica las mecánicas, las narrativas, las situaciones o la gestión de la mesa... Elimínalo de tu mesa. Así de sencillo.

Nosotros procuramos darte toda la información posible, para que luego cada uno se quede solo con la parte que enriquece sus partidas, y deseche el resto. Lo que ocurre es que lo que ayuda a cada uno suele diferir: hay mesas que agradecen tener un listado de especialidades, otras aprovecharán el glosario, otras los tipos de ataque o los tipos de defensa... Tú coge lo que te guste, el resto seguirá aquí, en estas páginas, esperando ser de ayuda a otras personas o a que tú vuelvas más adelante en busca de una experiencia diferente.

Las ayudas no piden pan. Esperan a que regreses, o a que alguien diferente las encuentre. Así que no te preocupes por todo lo que te sobre. Estará bien. Saldrá adelante. Tú céntrate en lo que te vale y olvida el resto.

Todo esto puede resultar un poco vago. Lo admitimos. Venga. Aquí van unos consejos más concretos que, esperamos, te ayuden a utilizar provechosamente los contenidos de este suplemento.

a) Qué hace es prioritario frente a qué es

Si te topas con algún concepto que te resulta difícil de entender, recuerda que es normal: estamos hablando de nociones técnicas. Aún intentando reducirlas a su explicación más sencilla resultan complicadas para quienes no tenemos formación técnica. ¿Entonces qué hago? te preguntarás. He aquí nuestro consejo: para tu partida, es más importante saber qué hace algo. Saber qué es o cómo funciona es secundario.

Te explicamos lo que queremos decir con un ejemplo de otro campo: cuando tus personajes se montan en un avión para volar de Buenos Aires a Madrid, lo que importa es que el avión les va a trasladar de una ciudad a otra surcando los cielos a través de la negra noche del océano Atlántico. Tiene poca -o ninguna- importancia, si tus personajes conocen o, en última instancia, comprenden los principios físicos que hacen que esa mole de metal se levante del suelo. Seguramente no conozcan ni siquiera los rudimentos del principio de Bernouilli ni del sistema de ecuaciones que se deriva de él, cuyas aplicaciones permiten volar a los Boeing 747. Pero ¿realmente importa? No. A tu partida le importa que tus personajes estarán en Madrid al día siguiente. O que hay un asesino en el avión. O que el piloto sufrirá un ataque al corazón. O, ya que estamos, que un ciberterrorista se hará con el control del piloto automático de la aeronave.

Para tu partida lo que importa no es tanto cómo funciona un *honey pot*, sino que sepas qué consecuencias tiene para tus jugadores: si caen en una, no podrán cumplir sus objetivos al colarse en un sistema ajeno y sus adversarios podrán averiguar mucho sobre ellos sin que se den cuenta. Eso es lo que importa para tu partida.

Céntrate en los efectos, narrativos y mecánicos, de los elementos técnicos. Casi todos estamos más cómodos con la práctica que con la teoría.

b) Coge la terminología y descarta todo lo demás

Ese es uno de los mejores usos que puedes dar a este suplemento. Quizá a ti y a tu mesa os sobren los detalles técnicos sobre tipos de ataque, métodos de defensa, etc. Quizá, como DJ, ya tienes una idea muy clara de cómo resolver una escena en que los PJ tratan de impedir que alguien que se ha colado en su ordenador les quite esas fotos tan comprometedoras o esos informes tan secretos. Perfecto. Usa tu sistema. Seguro que es más eficaz en tu mesa que cualquier otro que podamos proponerte.

Pero báñalo de términos técnicos. Estás moviéndote en un campo especializado, en el que los profesionales llevan a gala usar su propia jerga, no apta para profanos, y en el que quienes no han sido iniciados en los rudimentos de esa forma de magia moderna que es la informática no entendemos ni una palabra del aluvión de palabras extrañas -y, a menudo, en un idioma diferente al nuestro- con el que nos bombardean los especialistas. Entierra a tus jugadores en términos como ataque de denegación de servicio, *defacement*, requerir un token para descifrar el algoritmo de cifrado del código, etc.

El uso de un vocabulario especializado es una forma de inmersión, aunque no se utilice con precisión. O aunque sea inventado. Piensa en algunas de tus sagas de ciencia-ficción favoritas. Trata de

recordar alguno de los infinitos momentos en que los personajes comienzan a soltar una jerga técnica completamente inventada. ¿Qué utilidad crees que tiene en la narración? ¿Ayudarte a entender un fenómeno que es inventado a partir de palabrejas complejas que también son inventadas? ¡!!!No!!! La única función narrativa del vocabulario técnico de la ciencia-ficción, la *space opera* y otros géneros similares es generar inmersión: el vocabulario, la lengua, ayudan a construir mundos.

Tolkien lo sabía. Nombrar algo -en el sentido de dotarlo de un nombre- contribuye a hacerlo más sólido, tangible...

Es decir, real.

Así pues, usa vocabulario técnico. Con precisión, si puedes. O sin ella, si no te interesa asimilar qué es un ataque de ceguera o una bóveda electrónica. Pero usa esos términos. Ayudarán a que tus jugadores y tú os sumerjáis en la historia.

c) Ajusta la lente a tu interés

Cualquier campo técnico puede observarse de una forma tan general o tan detallada como se quiera. Lo que, como DJ, debes decidir es el nivel de detalle con el que quieres abordar cada cuestión. No tengas miedo en liquidar escenas a cuya resolución nosotros le dedicamos páginas y páginas. Si tu aventura no hace foco en cómo afrontar ese desafío, una única tirada es la mejor solución. Igualmente, no te cortes a la hora de descender a la minuciosidad al abordar cuestiones que para tu mesa sean vitales, aunque el suplemento las haya pasado por alto.

El telescopio es tuyo. Ajusta la lente para que muestre lo que quieres ver, ya sea una imagen general de una galaxia muy muy lejana o hasta el más mínimo detalle de la habitación del vecino - preferiblemente, lo primero-.

2.- Consejos variados

Aquí va un pequeño batiburrillo de ideas que a nosotros nos han resultado útiles a la hora de introducir el ciberespacio y la ciberseguridad en nuestras partidas.

a) Evita el efecto Lisbeth Salander

Vale. Empezamos con algo que a los fans de Steig Larsson les escocerá un poco. Nos explicamos. A lo largo de la primera novela en la que aparece el personaje de Lisbeth, *Los hombres que no amaban a las mujeres*, esta se adueña de la historia por la fuerza y el carisma que emana del personaje. Realmente, borra de la narración a su protagonista y es de ella de quien está pendiente el lector. A lo largo del tramo final de la narración, las capacidades de Salander como informática la muestran capaz de hacer prácticamente cualquier cosa a partir de sus conocimientos, idea que va a más a lo largo de las novelas posteriores de la serie. En un sentido narrativo, los conocimientos de hackeo de Lisbeth la convierten en un superhéroe, capaz de realizar actos que escapan a las posibilidades del resto de los mortales casi con completa impunidad.

No conviertas los conocimientos sobre ciberseguridad en un superpoder que permite a tus personajes obrar a su antojo.

No dejes que tus PJ utilicen sus capacidades en este campo para conseguir todo aquello que desean sin esfuerzo. Dinero, identidades, propiedades, información, venganza, alojamiento, fama... El

ciberspacio no debe ser un saco sin fondo virtual del que el personaje puede obtener, sin más, aquello que desea.

A veces, cuando uno es un martillo, es casi inevitable que todo parezca un clavo. Es una tentación lógica. Suele curarse después de que el DJ te diga: “Vaya, pues no era un clavo: era tu dedo”. Dicho de otra forma: haz que las consecuencias de sus actos salpiquen a los PJ si se comportan como si el mundo entero fuera un clavo.

Cada vez que se realiza una acción no autorizada, haz que el personaje sea consciente de que está asumiendo un riesgo. Que sepa que sus acciones tienen consecuencias. No que pueden tenerlas, sino que las tienen. Siempre. Puede que le descubran. Puede que pongan a alguien tras su pista. Puede que sus manejos en la Dark Web para conseguir un pasaporte falso le obliguen a contactar con gente muy poco recomendable. O puede que salga impune de haber robado el dinero de un incauto jubilado, pero ¿qué le pasa al jubilado? ¿Y al Karma de nuestro PJ? No va a mejorar, ¿verdad?

Ser un experto en ciberseguridad no es como ser Superman. El Hombre de Acero puede volar siempre que quiera y no pasa nada porque lo haga. No muere un hada en la Tierra de Nunca Jamás. Sin embargo, cada vez que tus personajes teclean código para una acción ilegítima en el ciberespacio, están jugándose su vida o su alma.

Desde el punto de vista de las mecánicas narrativas, hacer palpables los riesgos y posibles consecuencias de las acciones en el ciberespacio favorece que los personajes se comporten con cierta mesura a la hora de obtener recursos o de realizar acciones caprichosas aprovechándose de sus capacidades en el campo de las tecnologías informáticas. Ayuda, por tanto, a mantener la aventura dentro de unos cauces narrativos razonables.

b) Combina el ciberespacio con el mundo real

La resolución de acciones en el ciberespacio puede resultar muy reiterativa, ya que es fácil que derive en una sucesión de tiradas para superar las dificultades tecnológicas que plantean los adversarios de los PJ. Por ello, os sugerimos que en vuestras aventuras combinéis las acciones en el ciberespacio con acciones en el mundo real.

Tienes múltiples ejemplos de lo que queremos decir en la saga cinematográfica *Misión: Imposible*. Casi en cada film, el equipo que lidera Ethan Hunter debe obtener algo de un recinto de alta tecnología combinando el acceso a través del ciberespacio con un acceso físico a un lugar, equipo o punto concreto. Esto funciona muy bien también en las aventuras de rol: tu personaje debe penetrar el ordenador de la malvada supercorporación para demostrar que está vertiendo residuos en los ríos del país, pero para lograrlo debe acceder directamente desde el ordenador del CEO de la compañía, ubicado en la última planta de un gigantesco rascacielos de Shanghai.

Este tipo de enfoques permiten construir grupos con PJ diversos y que estos jueguen un papel en el desarrollo de los acontecimientos, en vez de limitarse a formar un corro y mirar por encima del hombro, con obnubilada admiración, como su informático teclea a velocidad de vértigo y hace saltar uno tras otro los cortafuegos de sus adversarios.

También tienen potencial narrativo las aventuras en las que la acción se desarrolla de forma paralela, de manera que los expertos en ciberseguridad y otro tipo de personajes aúnan esfuerzos con un mismo fin, aunque se encuentren físicamente en lugares y acciones diferentes.

Ejemplo: en una aventura, un terrorista se ha hecho con el control de un dron de combate del ejército norteamericano, y vuela sobre Washington en dirección a la Casa Blanca. El grupo de PJ trata de evitarlo, dividido en dos equipos: por una parte, desde las instalaciones del Pentágono, dos PJ especialistas en informática tratan de recuperar el control del dron; por otro, dos agentes del FBI recorren la ciudad reuniendo pistas que les permitan encontrar físicamente el escondrijo del terrorista.

c) Mazmorras virtuales

Muchos de los juegos que utilizan reglas para el ciberespacio diseñan este de la misma forma que una mazmorra en una aventura de fantasía clásica. Esto puede ser un recurso interesante si la aventura está focalizada en realizar intrusiones y si quieres invertir tiempo de juego en resolver paso por paso como tus PJ se abren paso a través de las defensas virtuales del equipo que asaltan.

Las salas del laberinto son sustituidas por nodos virtuales, pero a todos los efectos se comportan de la misma forma: los PJ pueden avanzar desde cada nodo a los que están conectados a él, como si de pasillos de un *dungeon* se tratara, y en cada una de las “salas” encontrarán un desafío, una trampa o un objeto -un código, una información...- que les sea de utilidad.

Por lo general, te recomendamos que uses este tipo de diseño solo en grupos en que todos los PJ puedan participar a la vez en la escena, o en los que pueda desarrollarse otra escena en paralelo. De lo contrario el foco podría pasar demasiado tiempo fijo en el personaje con capacidades para operar en el ciberespacio.

d) Aprovecha el rol on-line

Las partidas on-line generan unas condiciones muy específicas que puedes utilizar a tu favor en partidas con un importante componente de ciberseguridad, al establecer un paralelismo entre la situación de los personajes y la de los jugadores.

Imagina una aventura en el que los personajes son miembros de un colectivo de hacktivistas, cada uno de los cuales se encuentra en un lugar diferente del mundo, y que solo conoce a los demás a través de Internet. Si juegas la aventura on-line, esa puede ser exactamente la situación entre los jugadores, de modo que la inmersión en la aventura resulta sencilla. Incluso en un sentido físico, los jugadores estarán haciendo lo mismo que sus personajes: estar frente a la pantalla, frente al teclado, hablando con sus compañeros de aventura mediante un micro, escuchándolos a través de unos cascos...

Esa simbiosis entre la situación del jugador y la del personaje es capaz de generar inmersión inmediata, si se usa con habilidad por parte del DJ.

e) El ciberespacio está en todas partes

Recuerda que hoy en día hay aparatos electrónicos conectados a Internet que van más allá de los ordenadores. O, más bien, que son ordenadores en sí mismos. Nuestros teléfonos móviles tienen una capacidad computacional superior a la de los ordenadores con los que se gestionó la llegada del Apolo XI a la Luna; las tabletas son, en sí mismas, ordenadores. ¿Y qué decir del llamado Internet de las cosas? Electrodomésticos, sistemas de alarma, televisiones... La cantidad de tecnología que, en nuestra vida diaria, accede a Internet y, por tanto, es accesible desde Internet para un atacante, es muy grande.

No limites tus aventuras a interacciones con ordenadores y computadoras. Que los enemigos de los PJ traten de escucharlos a través de sus móviles. Que se hagan con el control de su Smart TV para enviarles un mensaje mientras ven su capítulo semanal de *Juego de tronos*...

3.- Resolución de acciones

Lo primero que debe tenerse en cuenta a la hora de resolver las acciones de *Karma* en el campo de la ciberseguridad es que no hay una forma correcta y muchas incorrectas de hacerlo. Estate tranquilo en ese sentido: puedes usar una u otra Capacidad a tu criterio. El sistema aguanta que utilices Inteligencia para resolver si tu PJ supera el cortafuegos para acceder al ordenador central de la NASA, y funciona igual de bien si le indicas que pruebe con Astucia, o incluso con Destreza, si consideras que la velocidad a la que teclee de forma simultánea en dos teclados al mismo tiempo es el elemento clave para superar el desafío.

Elige a tu gusto qué Capacidades se usan para cada tipo de desafío, pero sí es conveniente que ofrezcas a tus jugadores una explicación general al comenzar la partida, sobre todo si van a ser ellos quienes creen los personajes. Comprender cómo se va a resolver un tipo de problema en la partida les ayudará a diseñar personajes que sean competentes en aquello que les interese.

Una cosa que debes tener en cuenta es que las acciones relacionadas con la informática, más allá del mero nivel usuario de un equipo personal, requieren de formación específica y de conocimientos técnicos muy enfocados, por lo que, en términos generales, el personaje deberá poseer algún tipo de Especialidad relacionada con la materia para poder tratar de realizar una acción de ese tipo. Salvo que quieras ser muy preciso, deberías considerar que la Especialidad Informática capacita para cualquier tipo de acción relacionada con ciberseguridad, aunque no deberías considerar que puede activarse para obtener un +2 en acciones muy especializadas dentro de este campo.

Ejemplo: El personaje de Bernard tiene la Especialidad Informática y decide intentar colarse en el ordenador de una agencia de viajes para ver en qué fechas planea ausentarse el tipo en cuya casa su banda quiere robar. El DJ considera que Informática habilita a Bernard para efectuar la acción. Entonces Bernard le indica que quiere gastar un punto de Experiencia en activar la Especialidad para recibir un +2 a su tirada. El DJ lo rechaza: Informática supone que Bernard tiene conocimientos suficientes para intentar colarse en el ordenador, pero no que sea un especialista en ese tipo de acto. Frunciendo el ceño, Bernard pregunta qué Especialidad tendría que haber tenido para ello, y el DJ le indica que algo tipo Ciberseguridad, Hackeo, etc.

A continuación, te ofrecemos algunas sugerencias de cómo resolver las situaciones más frecuentes:

- Crear programas, códigos y, en general, todo lo que tenga que ver con la programación y el diseño de software -incluyendo malware-: Resuelve las acciones usando Inteligencia, añadiendo dificultad a medida que se le quieran añadir rasgos o características al programa o código que se están diseñando.

Ejemplo: Loris quiere crear un malware que, tras infectar el ordenador del blanco, registre todo lo que este teclee -es decir, un keylogger-. Dificultad Fácil para un especialista como Loris (+1); sin embargo, Loris quiere que el programa solo se active dentro de una semana -es decir, que sea una bomba lógica-, de modo que el DJ le añade un -1, aumentando la Dificultad. Si Loris quiere, además, enmascarar su rastro, el DJ podrá añadir un segundo -1, de tal forma que el modificar final a la tirada sea -2.

- Búsqueda de vulnerabilidades: aunque tendría lógica usar Inteligencia, creemos que Astucia es una Capacidad que define con más precisión el tipo de habilidad necesaria para, estudiando un sistema informático, encontrar sus puntos débiles.

- Perfilado o cualquier otra forma de reunión de información disponible públicamente en el ciberespacio: igualmente, recomendamos que uses Astucia para resolver este tipo de acciones.

- Reacciones en tiempo real: en ocasiones, un intruso y quién trata de contenerle se enfrentan en tiempo real para lograr cada uno imponerse al otro. En estos casos, te recomendamos que alternes las Capacidades, utilizando Intuición, puesto que la reacción en tiempo real, completamente improvisada, tiene mucho de arte; Destreza, simulando la velocidad a la que cada

uno de los partícipes es capaz de teclear sus órdenes, códigos, etc. Incluso puedes incluir tiradas de Percepción, en situaciones en que un personaje esté tratando de controlar lo que ocurre en varias pantallas al mismo tiempo.

- Creación o ruptura de códigos: el éxito o fracaso de un PJ cuando trata de crear un código para ocultar información, o trata de descifrar el código de su adversario para comprender un mensaje cifrado te recomendamos que lo determines con una tirada de Inteligencia.

La idea clave a la hora de resolver acciones es no utilizar la misma capacidad para todas y cada una de las situaciones. Esto resulta aburrido y ayuda a los jugadores a crear personajes ultra especializados, los cuales tienden a generar dinámicas desajustadas en la mesa de juego.

Este tipo de personajes pueden ser tan capaces en lo suyo que los problemas que se les planteen no supongan un verdadero desafío, lo que genera aburrimiento.

También se genera en ellos el ya mencionado efecto martillo: cuando eres un martillo, todo parece un clavo. De modo que pueden aparecer en mesa dinámicas por lo que el jugador trata de que personaje resuelva cualquier tipo de situación utilizando su superespecialización.

Por otra parte, el precio a pagar por su superespecialización es ser incompetentes en el resto de aspectos, lo que hace que queden marginados de cualquier desafío que no entre en su campo de maestría, estando casi siempre fuera de foco, o bien que estén condenados al fracaso constante cuando intenten cualquier cosa que no caiga dentro de su especialidad, dos fenómenos que perturban el equilibrio de la mesa de juego.

Como siempre, depende del tono de tu partida: si el ciberespacio resulta tangencial, no pasa nada por resolver las dos o tres acciones que puedan plantearse en la aventura con una tirada de Inteligencia; pero si la resolución de acciones de ciberseguridad va a ser constante, trata de alternar Capacidades sin perder de vista el sentido común.

CAPÍTULO VI: AYUDAS PARA PERSONAJES

1.- Rasgos

A continuación, te ofrecemos sugerencias sobre treinta rasgos diferentes que puedes incluir en partidas sobre ciberseguridad, ya que están conectados a los arquetipos propios de las narraciones de ficción ambientadas en ese género.

Evidentemente, no se pretende con ello transmitir la idea de que los estereotipos que aparecen en la cultura popular asociados a los especialistas en informática correspondan a una realidad empírica. Tan solo se pretende facilitar la tarea a jugadores y DJ que lo deseen, a la hora de construir personajes de ficción que incluyan elementos arquetípicos como parte de su diseño, utilizando Rasgos compatibles con estos estereotipos de ficción.

Nada impide que un analista de ciberseguridad, o un programador, no tenga ninguno de los Rasgos aquí descritos, siendo, por el contrario, un tipo acostumbrado a vivir en la naturaleza, amante de las artes marciales y con un cuerpo escultural gracias al tiempo que pasa practicando deporte al aire libre.

Lo más recomendable es combinar elementos arquetípicos con otros que no lo son. Es como mezclar dos sabores de helado: por un lado, la familiaridad del lugar común y, por otro, la personalización que aparta a cada personaje concreto del resto.

No es recomendable que un personaje tenga más de un Rasgo de la lista que sigue, en especial de los que se aplican de forma específica a las cibertecnologías, y en ningún caso debería tener más de dos, salvo que quieras que sea un auténtico cliché. No obstante, la decisión última es de tu mesa, y tan divertido puede resultar jugar con un informático que encaja al dedillo con Nedry, de *Parque Jurásico*, como con uno que no se parece en nada a la idea preconcebida del ciberespecialista.

Aquí tienes treinta ideas que pueden encajar con PJ para una partida en el que el ciberespacio sea relevante. Úsalas a tu gusto:

- **El mundo puede derrumbarse a su alrededor:** cuando el personaje se concentra en una tarea, es capaz de focalizar toda su atención en ella, hasta el punto de que puede llegar a parecer desconectado de cuánto le rodea.

- **Minucioso:** el personaje es detallista y comprueba cada detalle de las tareas que realiza. Muy apegado a sus rutinas, que sigue escrupulosamente, sobre todo en cuestiones relacionadas con su ocupación o sus aficiones.

- **Las máquinas son mejores que las personas:** el personaje se siente más cómodo trabajando con sus ordenadores y equipos informáticos que en situaciones de interacción social.

- **Antisistema:** el personaje está convencido de que el *status quo* de la sociedad es fruto de los intereses malignos de grandes entidades, ya sean los Estados, las corporaciones multinacionales o alienígenas ancestrales, por lo que siente un fuerte impulso de rebelarse ante dicho *status quo*.

- **Capacidad de abstracción:** el personaje se siente cómodo resolviendo problemas teóricos, analizando hipótesis o discutiendo sobre meros supuestos hipotéticos de carácter general. Tiene facilidad para las cuestiones que tienen que ver con campos abstractos -como la matemática, la filosofía...-. Por el contrario, cuestiones prácticas más mundanas, como cambiar una bombilla, no solo no revisten de interés para él, sino que pueden incluso suponer un desafío.

- **Obsesión por el anonimato:** el personaje mantiene una preocupación constante por el hecho de que pueda ser identificado en sus interacciones diarias, por lo que se ha convertido en un experto en moverse por la vida sin dejar huellas en sus actividades más cotidianas, si bien esta desconfianza constante puede generar elementos de comportamiento paranoide.

Si quieres expresar este rasgo de una forma más literaria, puedes describirlo, recurriendo a Orwell, como “El Gran Hermano te vigila”.

- **Tecnófilo:** el personaje es un apasionado de la tecnología. Le encanta la presencia de aparatos electrónicos en su vida diaria, incluso aunque no los necesite o los utilice muy

por debajo de las potencialidades. La tecnología le fascina, aunque no tiene por qué ser un experto en ella.

- **Orgullo Freak:** el personaje es lo que el resto de la sociedad define como freakie, y está orgulloso de ello. Informática, cómics, cine de serie de B, juegos de mesa o de rol son las cosas que le interesan y con las que se siente cómodo.

Vaya por delante que el nombre del rasgo es un pequeño homenaje al canal de YouTube Orgullo Freak, que Fada Joe, Pedro Calvo y otros roleros de pro han convertido en un verdadero templo del rol narrativo y de corte *indie*. Podéis acceder en sus contenidos en el siguiente enlace:

<https://www.youtube.com/user/OrgulloFreak>.

Si no lo conocéis, dejad lo que estáis haciendo -es decir, leer este suplemento-, y echad un ojo a alguna de las partidas que tienen colgadas, entre las que hay verdaderas joyas.

- **Enganchado a las redes sociales:** el personaje pasa gran cantidad de tiempo interactuando en varias redes sociales, conociendo al dedillo sus funcionalidades y sus protocolos sociales, moviéndose por ellas como pez en el agua. Por desgracia, el tiempo que dedica a las redes hace que descuide otros aspectos de su vida.

- **Youtuber:** el personaje tiene un canal de YouTube con cierto reconocimiento en el ámbito en el que se circunscribe, lo que lo otorga una popularidad limitada en su campo de actuación.

- **Cuchillo de palo tecnológico:** el personaje desarrolla una actividad profesional relacionada con la tecnología, pero las cosas que ve en su trabajo, en el que es competente, hacen que en su vida diaria trate de mantenerse lo más alejado posible de esas mismas tecnologías.

- **Preocupación por Skynet:** el personaje teme que el desarrollo tecnológico pueda convertirse en una trampa mortal para la humanidad y fenómenos como el desarrollo de la Inteligencia Artificial o el creciente papel de la tecnología en la vida diaria le preocupan sobremanera, por los que los ha estudiado en detalle, a fin de poder prevenir la catástrofe que él atisba en el horizonte.

- **Gremlin tecnológico:** el personaje es incapaz de resistirse a realizar bromas inofensivas utilizando para ello su conocimiento de la informática o de otras tecnologías similares.

- **Complejo de Peter Pan:** aunque ya tiene unos años, el personaje parece rechazar el proceso de maduración que llega con la edad. Sigue llevando un estilo de vida, unos hábitos, unas aficiones o un modo de vestir que son poco acordes con su edad, como si estuviera inmerso en una suerte de eterna adolescencia.

- **Creativo, o imaginativo:** el personaje tiene una gran capacidad para abordar y resolver problemas apartándose de los caminos trillados, y todo lo que suponga estimular esta capacidad creativa aumenta su implicación. Sin embargo, cualquier trabajo o situación que impliquen rutina, repetición o aburrimiento harán que el personaje la afronte con un nivel muy bajo de motivación.

- **Jefecillo de foro:** el personaje es un miembro destacado de alguna comunidad tipo foro, donde es una de las voces más activas y dominantes, con las afinidades y rencores que pueden llegar a despertarte en este tipo de ámbitos.

- **Cotilla cibernético:** el personaje está al tanto de los rumores y cotilleos que se mueven sobre la comunidad tecnológica en que se mueve, más en el sentido de chismes que en el de conocimiento tecnológico. Si quieres saber quién se lleva bien o mal con quién, que equipo se ha roto o qué romances virtuales están teniendo lugar, es tu hombre (o mujer).

- **Doble vida virtual:** el personaje se ha acostumbrado a llevar una doble vida completamente diferente, existiendo una dicotomía muy marcada entre su personalidad o vida real y la que adopta en el ciberespacio, donde actúa de una forma disociada con respecto al mundo físico (por ejemplo, con una identidad de género diferente, con una orientación sexual diferente, siendo tímido en la vida real y seductor en las redes sociales, etc.).

- **Usuario compulsivo:** el personaje tiene una fijación por un equipo tecnológico o una marca concreta, y es la que siempre utiliza. Es capaz de exprimir al máximo las capacidades de ese equipo, pero, por el contrario, sufre de una gran tensión y frustración si tiene que utilizar otros equipos.

- **Soberbia tecnológica:** el personaje tiene una gran formación en el campo de la tecnología y la ciencia en general, considerando que es la única forma de conocimiento que merece la pena. Todos los otros campos del conocimiento -pensemos, Dios no lo quiera, en la Historia o el Arte- son inferiores a las ciencias más puras y, de igual modo, las personas que no son capaces de comprender la tecnología son el equivalente moderno a las tribus perdidas que los exploradores europeos descubrían en regiones aisladas de tierras remotas en siglos pasados.

- **Urbanita:** el personaje no solo está acostumbrado a moverse en un entorno urbano, sino que lo ama y lo disfruta; para él, la naturaleza es, como decía un personaje de *Anticristo*, de Lars von Trier, “el templo de Satán”.

- **Se considera infravalorado:** aunque este concepto podría ser también una Visión Personal, lo cierto es que, si un jugador lo desea, puede emplearse como Rasgo para su personaje. Este considera que su valía y capacidad no han sido reconocidos por los que le rodean, lo que le generará cierta frustración y necesidad de reivindicarse, pero también la oportunidad para desplazarse, en ocasiones, por debajo de la línea del radar de quienes le rodean.

- **Fuera del tiempo:** el personaje no presta ninguna atención a cuestiones tales como la actualidad, la moda o las tendencias. Esto hace que, en ocasiones, pueda parecer desconectado del mundo en el que vive, pero, al mismo tiempo, le hace inmune a la presión o los efectos de ese tipo de fenómenos.

- **Alma de Joker:** algunas personas solo quieren ver arder el mundo, le dice Alfred a Bruce en *El caballero oscuro*. Ese es el caso de este tipo de personaje: poseen un rasgo destructivo en su carácter que los lleva a disfrutar sembrando el caos, aunque no haya una razón para ello.

- **Demasiado listo para su propio bien:** el personaje es inteligente y no para de demostrárselo a los demás con su actitud, su conversación, etc. Esto en ocasiones puede valerle el respeto de un oyente, pero también es una forma de conseguir la antipatía de muchos otros.

- **Jugador de equipo:** el personaje da lo mejor de sí mismo cuando permanece en segundo plano, apoyando al resto del grupo o del equipo. Por el contrario, le cuesta asumir responsabilidades y se resiente mucho de la presión cuando se convierte en el foco de atención, algo que tratará de evitar en la medida de sus posibilidades.

- **Un miembro leal:** el personaje siente una vinculación personal con la institución o la entidad para la que trabaja, considerando que es una gran organización y que es un motivo de orgullo y satisfacción pertenecer a la misma. Se mostrará reacio a aceptar hechos que choquen con esta visión y será difícil que rompa las normas y directrices que rigen su comportamiento como miembro de la institución, incluyendo el respecto por la jerarquía dentro de la entidad.

- **Hacker de primera generación:** el personaje, que ya tiene unos años, fue uno de los primeros que navegaban por el ciberespacio cuando Internet comenzó a cobrar fuerza, y sigue apegado en gran medida a los métodos y las historias de aquellos viejos tiempos. Seguramente, sus conocimientos y métodos hayan quedado, por ello, anticuados, pero sigue teniendo conocimientos y experiencias que pueden resultar de gran valor.

- **Especialista conocido:** el personaje tiene un largo historial de acciones a sus espaldas, por las que es conocido tanto por amigos y potenciales aliados como por enemigos y potenciales adversarios, incluyendo a las fuerzas del orden y a los especialistas de ciberseguridad. Por decirlo de forma simple, es un tipo fichado, para bien o para mal.



-Logo utilizado por el colectivo Anonymous-

- **Labrándose un nombre:** el personaje trata de ganar una reputación dentro del campo profesional o de actuación en el que se mueve. Eso lo hará proclive a asumir riesgos o a comportarse de forma algo individualista, pero también hará que esté muy motivado frente a desafíos que le permitan labrarse un nombre entre su comunidad.

2.- Uso de Especialidades genéricas de ciberseguridad

La ciberseguridad es un campo altamente especializado, como habrás podido comprobar de la lectura de las páginas anteriores, y el papel que vaya a jugar en tus partidas de *Karma* puede variar mucho. Creemos que, a efectos de juego, lo mejor es distinguir entre dos situaciones:

- Aventuras centradas en el mundo de la ciberseguridad.
- Aventuras en las que la ciberseguridad aparece, pero no es el elemento central de la trama.

En el primer caso, seguramente compense utilizar Especialidades precisas y detalladas, tal y como se ofrece en un epígrafe posterior, ya que la mayor parte de los personajes tendrán habilidades de ciberseguridad y, por tanto, se requerirá cierta precisión a la hora de definir las para diferenciar un personaje respecto de los demás. Para simplificar las Especialidades en este último caso, te aconsejamos que recurras a un modelo genérico, de forma que todo el abanico de posible especialización lo resumas en una o dos Especialidades generales, según el caso.

El modelo más sencillo sería dotar al personaje de la Especialidad Ciberseguridad, englobando en un solo término cualquier tipo de capacitación y conocimiento relativo con este campo. Aunque parezca demasiado simplista, lo normal es que resulte suficiente para cualquier aventura que no se centre de forma específica en el campo de la ciberseguridad.

Si te parece una reducción excesiva o si la historia que vas a jugar lo hace recomendable, puedes dotar de matiz a la Especialidad, sin ganar apenas en complejidad, dividiéndola en dos Especialidades diferentes:

- Ciberseguridad Activa: el personaje es especialista en realizar ataques, intrusiones y penetraciones en el ciberespacio.

- Ciberseguridad Defensiva: el personaje es especialista en proteger equipos, redes e instituciones de los ataques a través del ciberespacio.

Ciberseguridad, Ciberseguridad Defensiva y Ciberseguridad Activa serán especialidades suficientes en casi todas las misiones en que el ciberespacio pueda estar presente en una escena concreta, en un desafío al que se enfrenten los personajes o en una parte de su investigación, si no va a constituir el marco completo de la aventura.

El sistema dual de Especialidades Ciberseguridad Defensiva-Ciberseguridad Activa también soporta, desde el punto de vista mecánico, aventuras centradas en el ciberespacio. Si no quieres complicarte más, úsalo también en este caso, aunque perderás diferenciación entre los personajes. No obstante, hay mesas de juego en el que esta pérdida puede merecer la pena, en aras de una simplificación de las mecánicas.

Todo depende de lo que prefiráis.

3.- Especialidades de ciberseguridad

La informática en general y todo lo relacionado con la ciberseguridad en particular son viveros prácticamente infinitos para la inclusión de Especialidades para los personajes de Karma. A continuación, te ofrecemos una lista pensada para aventuras en las que

no sea suficiente con una Especialidad de corte genérico, como las que se sugieren en el epígrafe anterior.

Aquí van algunas propuestas:

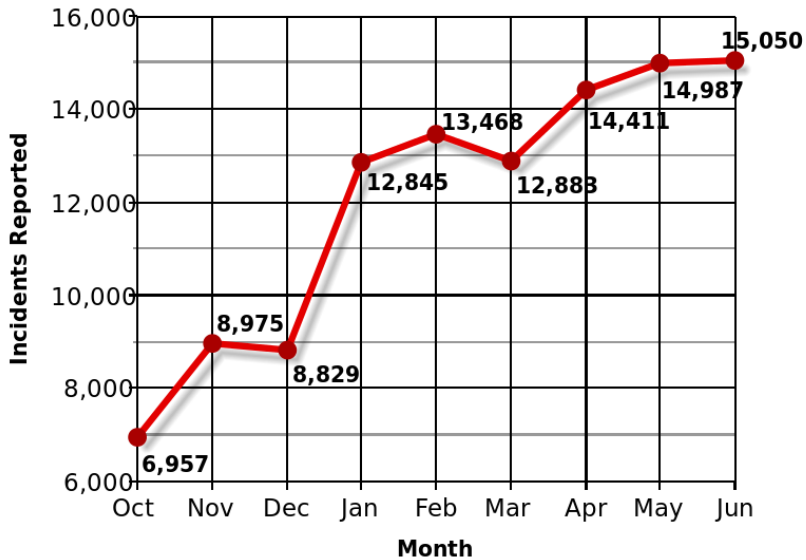
- **Dark web:** el personaje es un especialista en navegar por la Dark Web; sabe cómo encontrar sus directorios, como manejarse en sus páginas y foros y, en líneas generales, es capaz de operar con eficiencia en esa parte del ciberespacio.

- **Malware:** el personaje es un especialista en la creación de malware; por tanto, también será un especialista en el análisis del malware creado por otros.

Si lo deseas, puedes descomponer esta habilidad en dos, una para analizar los programas dañinos y otra para crearla, pero creemos que rara vez merecerá la pena tal grado de precisión en una partida, de modo que nuestra sugerencia es que permitas al personaje que tenga esta especialidad utilizarla en ambos sentidos.

- **Vulnerabilidades:** el personaje es especialista en detectar e identificar las vulnerabilidades de un equipo, sistema o red, ya sea para explotarlas o para subsanarlas.

- **Ingeniería social informática:** el personaje es un especialista en la manipulación del comportamiento de sus objetivos a través del ciberespacio, un verdadero experto en los denominados métodos de ingeniería social.



- Evolución del phishing entre 2004 y 2005-

- **Phishing:** el personaje es un artista del phishing, la comunicación con el objetivo para que él mismo te facilite sus claves, creyendo estar tratando con una entidad legítima.

Como se ha indicado anteriormente, el phishing es un modelo concreto de ingeniería social, por lo que, salvo que haya una poderosa razón de diferenciación entre PJ, lo mejor sería considerar que una persona que posee la Especialidad Ingeniería Social Informática puede utilizarla también para hacer phishing.

- **Denegación de servicio:** lo que al personaje se le da realmente bien son los ataques de denegación de servicio, y es en este tipo de acciones donde puede explotar al máximo sus talentos.

- **Contención de amenazas:** el personaje es especialista en combatir amenazas en curso, tanto para impedir las como para disminuir los daños que puedan producir. La Especialidad se puede aplicar durante el enfrentamiento en tiempo real con el agresor, no en acciones de prevención o posteriores al ataque.

- **Criptografía informática:** el personaje es experto en los programas de cifrado y descifrado que se utilizan para codificar el tráfico de información en el ciberespacio. Esta Especialidad se aplicaría a todo lo que tuviera que ver con el uso legítimo de los códigos y la información cifrada por parte de la persona -u organización- que envía el mensaje y de la persona u organización que es destinataria del mismo.

- **Ruptura de Códigos informáticos:** el personaje es experto de descifrar mensajes cifrados de los que no es el destinatario o emisor legítimo.

Por si la diferencia entre Criptografía y Ruptura de Códigos te resulta difusa, te pondremos un ejemplo:

Si el PJ fuera el agente ruso de nombre en clave Oso recibe un mensaje codificado procedente de la Central de Moscú, para decodificar su contenido y saber qué dice, utilizará su Especialidad de Criptografía, para aplicar de forma correcta los programas y claves de descifrado.

Sin embargo, si el PJ fuera un agente del FBI que ha interceptado el mensaje que Moscú envía al agente Oso, el personaje utilizaría su Especialidad Ruptura de Códigos Informáticos para tratar de decodificar el mensaje que los rusos envían a su agente infiltrado.

- **Análisis forense informático:** el personaje es especialista en estudiar, a posteriori, cómo se ha producido un ataque y qué daños ha causado.



- Sede del FLETC, centro estadounidense especializado en análisis forense en los años 80 y 90 del siglo XX-

- **Botnets:** el personaje es un especialista en trabajar creando redes de ordenadores que son controlados por su propia computadora, ya sea con conocimiento de los usuarios de las otras máquinas o, más probablemente, utilizándolos como “zombis”.

- **Intrusión cibernética:** el personaje es especialista en acceder a sistemas informáticos ajenos para después llevar a cabo acciones sobre ellos, como la implantación de malware.

- **Ciberespionaje:** el personaje es especialista en lograr acceder a redes y sistema cibernéticos sin que su intrusión sea detectada, lo que implica que su objetivo debe ser el mero acceso a información, no pudiendo utilizarse si el fin de la acción es causar un daño, alterar el equipo, etc.

- **Rastreo:** el personaje es especialista en rastrear a un atacante para lograr localizar geográficamente la ubicación del equipo del que ha partido un ataque o incursión.

- **Enmascaramiento:** el personaje es especialista en ocultar el origen de un ataque, una penetración o cualquier acto en el ciberespacio, impidiendo su localización y despistando a cualquier posible perseguidor a través de una maraña de servidores, botnets, etc.

- **Perfilado:** el personaje es especialista en trazar perfiles de personalidad, hábitos, consumo, opinión, etc. a partir del análisis de la actividad del objetivo en el ciberespacio.

4.- Personajes

En este epígrafe tienes trasfondos y estadísticas completas para cinco tantos personajes ficticios, que puedes utilizar como PJ o PNJ para tus aventuras. Todos son expertos en informática y, con poco trabajo, puedes adaptar su diseño para que se ajuste a la aventura que tengas en mente.

a) Masoud Daei

Masoud Daei es uno de los más talentosos miembros del Tarh Andishan, un grupo de ciberespecialistas que, según se dice, fue creado por el gobierno de Irán para devolver a los enemigos de la república islámica el cibergolpe asestado a través de Stuxnet.

Daei es un hombre joven y apuesto, que encaja poco en la imagen preconcebida que pueda tenerse de un agente del gobierno iraní. Se considera un buen musulmán, aunque dista de ser un fanático y, como los creyentes de muchas otras fes, a veces la comodidad, el deseo o la pereza pueden más que sus obligaciones religiosas.

Lo que Daei sí es un patriota convencido, que detesta el modo en que los occidentales tratan a su país, menosprecian su cultura, estigmatizan su religión e ignoran su historia. Por ello, disfruta cada vez que él y su grupo dan a Occidente una lección de humildad y les enseñan que Irán es un país que debe ser respetado.

Se formó en prestigiosas universidades europeas, residiendo en Alemania durante sus años de estudio, por lo que es perfectamente capaz de desenvolverse en Occidente, donde conserva algunas de las amistades que hizo durante el tiempo que vivió allí. De hecho, viaja a Europa con cierta frecuencia, donde se permite disfrutar de ciertas libertades que no son admitidas en Teherán, su lugar habitual de trabajo y residencia.

Estadísticas:

- **Concepto:** ciberespecialista al servicio del gobierno de Irán.

- Rasgos:

- Ama a su despreciado país.

- En su interior, admira la vida occidental.

- Mujeriego.

- Visiones:

- Personal: Soy un hombre moderno.

- Vital: Occidente desprecia y explota al resto del mundo.

- Especialidades:

- Seducción.

- Malware.

- Penetración informática.



- Capacidades:

- Físicas: Fuerza +1, Destreza +1, Agilidad +1, Percepción +0.

- Mentales: Inteligencia +1, Astucia +1, Intuición +1, Voluntad +0.

- Sociales: Carisma +1, Negociación +1, Intimidación +0, Manipulación +1.

- Energía: 14.

- Pulsiones:

- Idealismo +2

- Orgullo +1

- Hedonismo +1.

- Lujuria +1

- Sociabilidad +1.

b) Dawn Wood

Dawn es una persona tranquila y callada, que se sienta cada mañana en su mesa de trabajo con su taza de té y que habla siempre en un tono sereno, por muy enfadada que esté. Resulta fácil olvidar lo condenadamente buena que resulta en su trabajo, analista de ciberseguridad.

Dawn pasa horas y horas buscando información en la red, conectando con líneas invisibles puntos que todo el mundo puede ver pero que solo ella relaciona, y es un as cuando realiza reconstrucciones forenses de ataques en el ciberespacio.

Trabaja para una gran empresa de seguridad, a la que contratan empresas aún más grandes para velar por la seguridad de sus sistemas y para detectar amenazas potenciales a sus intereses en el confuso flujo de la red.

Aunque le gusta su trabajo, Dawn tiene una vida que empieza cuando apaga su ordenador y abandona su oficina. Vive en un apartamento con su mascota -¿gato? ¿perro? ¿uno de cada? Elige a tu gusto-, se reúne con frecuencia con sus amigos y, en resumen, lleva una vida normal: el trabajo no ha absorbido el resto de su existencia.

Estadísticas:

- **Concepto:** Analista de ciberseguridad.

- Rasgos:

- Locura por su mascota.
- Jugadora de equipo.
- La vida no termina en una pantalla.

- Visiones:

- Personal: Soy una buena persona.
- Los animales son mejores que la mayor parte de las personas.

- Especialidades:

- Perfilado.
- Análisis forense informático.
- Trato con mascotas.



- Capacidades:

- Físicas: Fuerza -1, Destreza 0, Agilidad 0, Percepción +1.

- Mentales: Inteligencia +2, Astucia +2, Intuición +0, Voluntad +2.

- Sociales: Carisma +1, Negociación +1, Intimidación -1 Manipulación +1.

- Energía: 12.

- Pulsiones:

- Conocimiento +1.

- Curiosidad +1.

- Generosidad: +1.

- Compasión: +1.

- Espiritualidad: +1.

c) Lewis Smith

Lewis ha tenido que buscarse las habichuelas desde muy joven, trabajando en varios empleos mal remunerados para pagar sus estudios de informática. Comenzó trapicheando a través de plataformas como Wallapop y más tarde descubrió que había un lugar, más oscuro, profundo y tentador, donde se podía hacer más dinero comprando y vendiendo lo que fuera que la gente quisiera encontrar. De la noche a la mañana, casi sin darse cuenta, se convirtió en un navegante de la Dark Web.

Lewis no vende nada en concreto. Tampoco compra nada en concreto. Es una de esas personas que se ocupa de conectar a la gente que quiere algo con la gente que vende ese algo. A veces se lleva un pellizco. Las más de las veces. A veces, es solo un favor que hace a gente que ya se lo devolverá más adelante.

Aunque intenta mantener sus manos limpias respecto de determinados materiales que se mueven por la Dark Web, Lewis no siempre lo ha conseguido. No obstante, prefiere mantenerse lo más lejos posible de los negocios más sucios y truculentos. Por ejemplo, no recurre a Lewis para transacciones que impliquen la muerte de alguien. Ahora bien, si buscas drogas, compañía, una mascota exótica o algún objeto de coleccionista, Lewis podrá decirte donde encontrarlo.

Lewis cree que ya tiene suficiente dinero como para salir de la Dark Web y cumplir su sueño: crear su propia empresa informática, dedicada al desarrollo de videojuegos. Sin embargo, está aprendiendo algo que casi todos los que han ganado dinero con negocios ilegales terminan por descubrir: es más fácil entrar que salir.

Estadísticas:

- **Concepto:** intermediario de la Dark Web.

- Rasgos:

- Las muertes son un mal negocio.
- Pronto dejaré este *business*.
- Todo el mundo me conoce.

- Visiones:

- Personal: Puedo dejarlo cuando quiera.
- Vital: Todo está en venta.

- Especialidades:

- Dark Web.
- Ingeniería Social.
- Economía.



- Capacidades:

- Físicas: Fuerza +0, Destreza +0, Agilidad +0, Percepción +2.

- Mentales: Inteligencia +1, Astucia +2, Intuición +0, Voluntad +0.

- Sociales: Carisma +1, Negociación +1, Intimidación +0 Manipulación +2.

- Energía: 13.

- Pulsiones:

- Ambición: +1.

- Codicia: +1.

- Lujuria: +1.

- Prudencia: +2.

d) Tom Borrrough

Tom robaba a los ricos y se lo daba a los pobres. Bueno, no a todos los pobres. A uno en concreto. A él mismo. Ramsonware, phishing y, su favorito, buscar la gran ballena blanca, esos ejecutivos que gobiernan el mundo, y golpearles en el corazón... Es decir, en el bolsillo. Ah, chicos, eso sí que era vida. Robar a los ricos era su límite moral, lo que le permitía dormir por las noches. Y es que, aunque era un ladrón, Tom tenía una conciencia bastante molesta.

Luego vino el FBI, claro. Nadie puede robar a los ricos durante demasiado tiempo. No en este mundo. Si quieres tener una larga carrera, roba a los pobres. Pero Tom no quería robar a los pobres. Había visto a muchos a lo largo de su vida. Si no fuera por sus becas, hubiera sido uno de esos pobres tipos que puedes ver, consumiendo sus vidas en empleos que detestan. Y eso los que tienen un empleo que detestar...

Dentro de lo que cabe, Tom tuvo suerte. A veces, es lo que se dice cuando eres bueno en lo tuyo. Qué tienes suerte. En fin.

Mucha gente mataría por la elección que le dieron los federales: veinte años en una prisión federal o un sueldo como asesor del FBI para luchar contra cibercriminales. Así que Tom se convirtió en Pat Garrett. De hecho, ese es el Nick que utiliza en redes: el forajido que se convirtió en agente de la ley para capturar a sus amigos. El mundo cambia, Billy, piensa, con cierta nostalgia de los buenos viejos tiempos, cada vez que se sienta frente a sus pantallas para capturar a los malos...

Estadísticas:

- **Concepto:** Consultor al servicio del FBI.

- Rasgos:

- Roba a los ricos y quédatelo tú.
- No siempre ayudé a los polis.
- El mundo puede derrumbarse a su alrededor.

- Visiones:

- Personal: Soy un hombre libre.
- Vital: Elige el mal menor.

- Especialidades:

- Phishing (Ingeniería social, si quieres hacerlo más amplio).
- Dark Web.
- Cinefilia.

- Capacidades:

- Físicas: Fuerza +0, Destreza +1, Agilidad +1, Percepción +1.
- Mentales: Inteligencia +1, Astucia +2, Intuición +1, Voluntad +0.
- Sociales: Carisma +1, Negociación +1, Intimidación +0 Manipulación +1.



- **Energía:** 13.

- **Pulsiones:**

- Codicia +1.

- Hedonismo +1.

- Sociabilidad +1.

- Compasión +1.

- Orgullo +1.

e) Chiara dell Monte

La verdad es un arma termonuclear. Es capaz de derribar los castillos de mentiras que construyen los poderosos para mantener sumisas a las masas. Por eso Chiara creó un colectivo de hacktivistas y lo llamó NuclearTruth. En los ratos libres que les dejan sus trabajos de ocho horas en empresas a las que odian, los miembros del colectivo difunden verdades incómodas robadas de los cajones oscuros de empresas y gobiernos.

Chiara tiene un héroe, Julian Assange, y una fe inquebrantable en que el mundo puede cambiar. A mejor, incluso. Solo requiere un pequeño empujón. Es decir, de los esfuerzos de una vanguardia de rebeldes que, con sus acciones, sean capaces de levantar a las masas dormidas, arrancándolas de la pasividad en que les ha sumido el capitalismo. Si supieran como se juega con sus vidas, como son

apostadas en mercados de futuros por gente que vive vidas que los demás ni siquiera pueden soñar, saldrían a las calles y tomarían las riendas de su destino.

Chiara tiene veintidós años.

Chiara es intensa, idealista, apasionada. Te fascina o te agota, y si te agota la evitas, de modo que la mayor parte de la gente con que se codea son personas a las que fascina.

Pero Chiara tiene un secreto: es una niña rica. Su padre es un alto cargo de una multinacional. No se lo ha contado a nadie, pero se crió rodeada de los privilegios que la situación económica de su familia podía facilitarle. Teme qué podría pasar en NuclearTruth si los demás miembros del grupo lo supieran algún día. Incluso tiene pesadillas con ello.

Estadísticas:

- **Concepto:** Hacktivista niña rica.

- Rasgos:

- Intensa.

- Temor a que su vida real sea descubierta.

- La quieres o no la soportas.

- Visiones:

- Personal: Soy una líder.
- Vital: la gente puede despertar.

- Especialidades:

- Denegación de servicio.
- Finanzas.
- Enmascarar su identidad informática.

- Capacidades:

- Físicas: Fuerza +0, Destreza +0, Agilidad +1, Percepción +1.

- Mentales: Inteligencia +1, Astucia +1, Intuición +1, Voluntad +1.

- Sociales: Carisma +2, Negociación +0, Intimidación +0 Manipulación +2.

- Energía: 13.



- Pulsiones:

- Idealismo: +2.
- Ambición: +1.
- Romanticismo: +1.
- Orgullo: +1.
- Audacia +1.

CAPÍTULO VII: ACCIONES DE ATAQUE Y DEFENSA

1.- Tipos de acciones agresivas

A lo largo de una aventura con un importante componente de ciberseguridad, tus PJ podrán llevar a cabo múltiples tipos de ataque, o bien enfrentarse a ellos. Aquí te ofrecemos algunas posibilidades.

a) Ataques de denegación de servicio

En este tipo de ataques, lo que el actor busca es colapsar el funcionamiento de un servidor o página web, enviándole tal volumen de comunicaciones que no sea capaz de atenderlas y “atasque” todo el sistema, del mismo modo que ocurre con el tráfico de vehículos: si envías suficientes vehículos por la misma carretera, tarde o temprano se atascará y ninguno se moverá o lo hará tan despacio que desesperará a los usuarios.

Por tanto, la base de un ataque de Denegación de Servicios es dirigir una gran cantidad de tráfico cibernético al punto que se quiere colapsar -pongamos por caso, la página de venta on-line de una peletería-. Para ello, es frecuente recurrir a una botnet, de modo que el

actor controla múltiples equipos que no son suyos y que envían tráfico al objetivo hasta saturarlo.

En términos de juego, te recomendamos que sigas estos dos pasos:

- El actor debe crear una botnet que le permita generar un volumen de tráfico susceptible de colapsar el objetivo. La dificultad dependerá del blanco: colapsar el ordenador de la web de la copistería de tu barrio quizá no sea muy complicado, pero colapsar el servidor de una multinacional requerirá mucho más tráfico. También debería tenerse en cuenta el tiempo invertido: si se dedican tres meses a preparar la botnet, tener éxito será más fácil que si solo se dispone de unas pocas horas.

Este paso te lo puedes saltar si el atacante puede reunir un número de colaboradores voluntarios lo bastante elevado que generen, de forma consciente y voluntaria, el tráfico contra el blanco. Podría darse este caso en el caso de campañas con motivaciones políticas o ideológicas, que movilizan a miles de personas por todo el mundo, o también en el caso de que el atacante sea un Estado o una corporación que tenga esos recursos a su alcance sin necesidad de crear una botnet.

- Resuelve el ataque de Denegación de Servicio propiamente dicho, utilizando los resultados de la creación de la botnet como modificadores: un Éxito podría dar +1 a la tirada, un Éxito Parcial un +0 y un Fracaso un -1 o bien hacer imposible el ataque, según estime el DJ.

En base al resultado de la acción, lo habitual será que el Éxito suponga el bloqueo o caída de la página; el Éxito Parcial podría suponer que el servicio se ve ralentizado y sufre problemas, pero no llega a interrumpirse, o bien que cae por completo por un periodo de tiempo corto. Como en todo Éxito Parcial, puedes dar a elegir al jugador entre las dos opciones.

Ejemplo: el hacktivista Rock Forever decide lanzar un ataque de Denegación de Servicio contra la web de venta de entradas de Gran Macho Alfa, un célebre cantante de reguetón. Para ello, primero debe de hacerse con el control de una botnet, tarea a la que el DJ le asigna una dificultad de +0, teniendo en cuenta que la web es bastante grande, pero Rock Forever ha dedicado una semana a montar su botnet. Con un resultado de 9 en su tirada, el Éxito supone que el DJ da un modificador de +1 a la siguiente parte del plan del Rock Forever: realizar el ataque el día en que salen a la venta las entradas del concierto de Gran Macho Alfa. De modo que el jugador lanza el dado y obtiene un 7, lo que da un resultado final de 8: Éxito Parcial. El DJ da a elegir a Rock Forever si prefiere problemas continuos y ralentización de la página o bien una caída breve, pero completa. Escoge la primera opción, y se sienta a disfrutar como los foros y las redes sociales se llenan de comentarios incendiarios sobre lo mal que ha funcionado la web y la poca previsión de los organizadores. Algo es algo...

b) Secuestro de sesión

En un secuestro de sesión, el atacante se aprovecha del acceso al sistema de un usuario legítimo, que entra con su propia contraseña en el entorno al que quiere llegar el atacante. Una vez el usuario legítimo ha introducido la clave y se encuentra dentro del entorno protegido, el atacante toma el control de la sesión iniciada, pudiendo realizar dentro del sistema cualquier acción para la que estuviera autorizado el usuario legítimo cuya sesión ha “secuestrado”.

En el caso de que el dueño de la sesión secuestrada no tenga conocimientos de ciberseguridad, no será capaz de entender qué está pasando, pero si tiene capacidad al respecto, podría intentar rastrear o contener el ataque, luchando por recuperar el control e impidiendo así que el atacante se salga con la suya.

c) Búsqueda de vulnerabilidades

Los personajes que quieran llevar a cabo una penetración en un sistema informático seguramente intenten primero llevar a cabo una exploración que les permita detectar vulnerabilidades, para averiguar cuál es la mejor vía para acceder al equipo o atacarlo. Normalmente, se usan programas específicos para tantear los sistemas y buscar las debilidades de la seguridad, existiendo algunos disponibles en código libre, para cualquiera que quiera usarlos, como el programa llamado Satán.

Desde el punto de vista de la mecánica de juego, si una búsqueda de debilidades tiene Éxito, otorga un modificador positivo a cualquier ataque posterior contra el sistema. Por el contrario, un Fracaso podría poner sobre aviso a la ciberseguridad del objetivo y aumentar la dificultad de la incursión posterior, o que, cuando esta se produzca, el atacante encuentre algún tipo de trampa, como un *honey pot*, o con un equipo de ciberseguridad listo para contenerle y rastrearle.

d) Enmascarar el rastro

Los atacantes no quieren ser identificados ni localizados, por lo que tratan de cubrir las huellas que dejan durante sus acciones. A esto nos referimos con el término enmascarar el rastro: el intento de impedir que alguien pueda identificar la ubicación, geográfica o cibernética, del personaje que ha llevado a cabo una acción concreta en el ciberespacio,

utilizando lo que los especialistas denominan “técnicas avanzadas de evasión”.

Debe tenerse en cuenta que la acción hace referencia solo a cubrir las huellas informáticas, no cualquier otra pista que haya dejado el personaje durante sus acciones.

e) War Chalking

¿Alguna vez has observado esas extrañas marcas de tiza en la pared de un edificio, mientras caminas por tu ciudad? Bien podrían ser el resultado del *war chalking*, una práctica consistente en marcar con tiza el exterior de edificios donde se han detectados conexiones de red inalámbricas inseguras, de modo que otros puedan reconocerlas y, ubicándose en las inmediaciones, utilizarlas.

Esta práctica tiene muchas variantes, cada una de las cuales recibe su propio nombre. Por ejemplo, cuando la búsqueda de redes inseguras se realiza desde un coche que circula a baja velocidad, para permitir al pasajero explorar las redes de la zona, se denomina *war driving*.

Si uno de tus personajes busca una red inalámbrica a la que acceder mediante estos sistemas, la dificultad de la tirada dependerá de la naturaleza de la zona. En lugares con muchos espacios públicos, -cafeterías, centros comerciales, estaciones, etc.-, será relativamente fácil encontrar redes abiertas o poco protegidas. En barrios donde se concentren edificios oficiales o grandes multinacionales con preocupaciones sobre seguridad informática será más difícil hallarlas. Igualmente, será más fácil encontrarlas en entornos hipertecnificados,

como el Tokyo del siglo XXI, que en zonas de menor desarrollo, como una aldea del altiplano boliviano.

f) *Watering Hole*

El ataque de *watering hole*, a los que en castellano a veces se menciona como ataques de abrevadero, consiste en infectar una web que, sabemos, es frecuentada por el verdadero objetivo del ataque. De esta forma, el blanco resulta contaminado por el malware durante una visita a su web habitual, evitándose realizar una penetración en el equipo del objetivo. De ahí toma su nombre: recuerda esas imágenes de los documentales sobre la sabana africana en los que puede verse a los cocodrilos esperando en las escasas charcas a las que, tarde o temprano, sus presas se acercarán a beber...

Desde el punto de vista de juego, los personajes deben averiguar qué páginas y sitios web visita su blanco, para, a continuación, realizar un ataque sobre ese sitio e infectarlo con el malware que, más adelante, esperan que infecte a su objetivo. Deberán, por tanto, superar tres desafíos:

- Identificar la web que frecuenta el blanco.
- Infectar la web frecuentada por el blanco.
- Lograr que el blanco se infecte sin darse cuenta.

g) *Ataque de phishing*

La pesca, para un ciberdelincuente, consiste en suplantar la identidad cibernética de una entidad -principalmente, un banco- y comunicar con los clientes de esta como si se tratara de la entidad legítima, solicitándoles datos de acceso y clave, por lo general con una

excusa tipo “necesitamos verificar su identidad para seguir operando”, o “estamos realizando una comprobación de seguridad”. Si el cliente pica el anzuelo, entregará a los delincuentes sus claves, permitiéndoles operar con su dinero hasta que se dé cuenta de lo sucedido.

Una forma específica de este ataque es el llamado *whaling* o caza de ballenas, también denominado *spearphishing*. En estos casos, los blancos no son masivos, como suele ocurrir en el *phishing*, sino que se orientan específicamente hacia individuos concretos de gran peso, como ejecutivos de alto nivel.

Por lo general, un ataque de *phishing* en el juego tendrá múltiples blancos y la finalidad de reunir fondos, por lo que puedes resolverlo con una tirada genérica que determine, de un solo golpe, el balance de conjunto de toda la operación. En el caso de *whaling*, seguramente sea recomendable dedicarle algo más de detalle, ya que la mera elección del ataque implica que se ha buscado a un blanco o grupo de blancos muy concreto, adaptar el modelo de ataque y, por lo general, buscar datos más allá de unas simples claves para manejar dinero -por ejemplo, la clave de seguridad que permite acceder a un sistema determinado-.



Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

<http://www.trustedbank.com/general/custverifyinfo.asp>

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

-Ejemplo de mail de phishing-.

h) Perfilado

El perfilado no es un ataque en sentido estricto, aunque puede ser el primer paso para uno. Consiste en intentar deducir la personalidad, hábitos y comportamientos del objetivo a partir del estudio de su actividad en el ciberespacio. Puede ser un fin en sí mismo -reunir información sobre un individuo- o puede ser el primer paso para un ataque cibernético posterior.

Por ejemplo, un ataque de *whaling* o de *watering hole* casi siempre irán precedidos de la reunión de información detallada sobre el blanco, lo que bien pudiera hacerse mediante un perfilado.

i) Ataque de *pharming*

El *pharming* es un tipo de ataque destinado a obtener las claves bancarias de las víctimas. Cuando su equipo se ve infectado, al teclear la dirección de su banco, el malware reescribe la dirección IP a la que quiere ir el usuario y le desvía a una web falsa que simula ser la de la institución bancaria, de modo que el usuario introduce sus claves ignorando que se las está facilitando al delincuente.

Aunque está concebido como un fraude bancario, el *pharming* puede utilizarse para conseguir contraseñas de todo tipo de instituciones. El personaje debe tener en cuenta que, tarde o temprano, el usuario legítimo se dará cuenta de que no está en la página original y cambiará lo antes posible las claves, por lo que el agresor dispone de un tiempo relativamente corto para actuar, aunque en el caso de las operaciones bancarias suele ser margen suficiente para que el delincuente logre transferir dinero a sus propias cuentas.

j) Ataque de fuerza bruta

Con este nombre se conoce a un tipo de ataque cibernético que trata de forzar el acceso a un entorno protegido por una clave probando todas las combinaciones posibles.

Dicho de otra forma, si tuviéramos una clave formada por cinco números, el ataque de fuerza bruta consistiría en probar cada una de las cien mil combinaciones posibles entre el 00000 y el 99999.

Este tipo de ataques requieren mucho tiempo, ya que el programa atacante realiza pruebas combinación por combinación, y dependiendo del número de elementos de la clave y del tipo de caracteres posibles - letras, números, signos ortográficos, mayúsculas, minúsculas...- el tiempo necesario para descifrar una clave mediante un ataque de fuerza bruta puede llegar a ser de cientos de años.

Una variante más refinada del ataque de fuerza bruta es el ataque de diccionario, en la cual el programa trata de desentrañar la clave utilizando una por una todas las palabras del diccionario de la lengua que se cree que utiliza el usuario legítimo. No obstante, este método solo es eficaz en el caso de contraseñas con un muy bajo nivel de seguridad y que no utilizan ni números ni otros tipos de caracteres.

k) Basuring

Penetración en un equipo o sistema que tiene por blanco la papelera de reciclaje y otros elementos del sistema donde se almacenan elementos o materiales borrados, con el fin de acceder a sus contenidos y reunir datos e información de utilidad para el asaltante.

l) Bomba lógica

Las bombas lógicas son un tipo de malware que se activa cuando se cumple una condición previamente establecida. Esta puede ser de cualquier tipo: una fecha, tras un número concreto de encendidos o apagados del equipo, un número de días determinado a partir de la fecha de infección...

Esto implica que el malware permanece un tiempo inactivo dentro del equipo infectado, por lo que, a efectos mecánicos, una vez la bomba lógica haya sido instalada, sería conveniente realizar al menos una tirada para determinar si la ciberseguridad ha sido capaz de detectar y eliminar la amenaza en el tiempo que ha pasado entre su instalación y su activación.

Por lo general, si han sido los PJ quienes han instalado la bomba lógica, el momento más adecuado dramáticamente para efectuar esa tirada es el instante en el que el malware debería activarse.

¿Recuerdas la imagen final de *El Club de la Lucha*, con Edward Norton y Helena Bonhan-Carter contemplando los rascacielos en el horizonte? Si su bomba hubiera sido lógica, ese es el momento preciso en el que David Fincher debería haberles pedido que tiraran los dados para ver si habían tenido éxito.

m) Ataque de ceguera

Con el término ataque de ceguera se hace referencia al intento de burlar un sistema de detección inundándolo con elementos que contienen el marcador que está programado para detectar, de tal manera que la avalancha de positivos y de alarmas vuelva inútil el sistema. El éxito de este tipo de ataque, como en el caso de los ataques de denegación de servicio, depende de conseguir generar un volumen de mensajes tal que sea capaz de saturar el sistema de detección.

Estos ataques funcionan de la misma forma que los señuelos chaff que utilizan los aviones de guerra, lanzando al aire miles de tiras de aluminio que, en las pantallas de radar enemigos generan la misma señal que un avión, enmascarando la verdadera aeronave entre cientos de otros contactos positivos, que no son más que cebos.

n) Defacement

Cuando se “desfigura” un blanco, a lo que se hace referencia es a que el ataque ha alterado la parte visible al público de la web contra la que ha lanzado, generalmente de una forma dañina o humillante para el propietario de la web.

ñ) *Drive-by*

Los *drive-by* son un tipo de malware que infecta a las víctimas por el mero hecho de visitar la página web donde se encuentra el malware, sin necesidad de que lleven a cabo ninguna otra acción. Se

trata del tipo de programas que, habitualmente, se utiliza en los ataques de *watering hole*.

o) DNS poisoning attack

En este tipo de ataques, el incursos altera el buscador de Internet que usa el blanco, de tal modo que los resultados de sus búsquedas dirigen a la víctima hacia las páginas que quiere el atacante. Con frecuencia, se trata de páginas infectadas con *drive-by* u otros tipos de malware.

2.- Acciones defensivas

En una aventura, tus personajes también podrían encontrarse del lado de la ciberseguridad, tratando de impedir con sus acciones que los ciberdelincuentes logren sus objetivos. Aquí tienes un listado de algunas de las acciones que podrían emprender para ello.

a) Rastrear

En el contexto de este suplemento, rastrear sería el intento de un especialista en ciberseguridad por tratar de localizar geográficamente el origen de un ataque, ya sea en tiempo real o bien reconstruyéndolo a posteriori una vez que ha ocurrido.

La dificultad de resolución debería verse influida por las capacidades del atacante para enmascarar su rastro y por el éxito de sus acciones en este sentido.

b) Contener

En términos de juego, contener sería tratar de bloquear un ataque en curso para impedir que tenga éxito, impidiéndole causar daños en el sistema o acceder a información confidencial.

Dado que en estas situaciones atacante y ciberseguridad se están enfrentando en tiempo real, tratando cada uno de superar en habilidad a su oponente al mismo tiempo, la dificultad de las tiradas deberá establecerse en base a una comparación de la capacidad de cada uno.

c) Ingeniería inversa

La ingeniería inversa, en general, consiste en deducir el proceso de construcción de algún tipo de mecanismo a partir del objeto terminado, siendo una forma de obtener conocimiento tecnológico al que no se había llegado hasta entonces por sus propios medios.

Veamos un ejemplo histórico: durante la Primer Guerra Púnica, en el siglo III a. C., Roma, que era una potencia cuya fuerza militar era sobre todo terrestre, se enfrentó a Cartago, cuya fuerza derivaba de su dominio de los mares. Los romanos necesitaban una flota para enfrentarse a los cartagineses, pero no tenían experiencia en construcción de buques y sus diseños eran inferiores a los de sus enemigos. Pero la suerte -o los dioses-, se pusieron del lado de Roma y una trirreme cartaginesa fue capturada intacta por Roma. Los romanos enviaron a sus mejores ingenieros a estudiar el navío y, a partir del mismo, utilizando ingeniería inversa, dedujeron el mejor modo de fabricarlo, de forma que, en pocos meses, los astilleros romanos botaron una flota de varios cientos de naves.

En términos de ciberseguridad, cuando un personaje realiza ingeniería inversa, analiza un malware o cualquier otro programa elaborado por un adversario, con alguno de estos objetivos:

- Descubrir su propósito.
- Descubrir la mejor manera de contrarrestarlo.
- Reunir información sobre su creador.

Según el grado de Éxito que logre el personaje, puedes darle más o menos información de cada campo, o limitar lo que averigua a un campo.

Si lo deseas, puedes permitir usos más amplios de la ingeniería inversa. Por ejemplo, podría utilizarse por un atacante que, descomponiendo y analizando las medidas de protección de un sistema, quisiera averiguar cosas sobre quién lo ha diseñado, qué es lo que protege, etc.

d) Análisis heurístico

Este tipo de análisis trata de localizar malware revisando el estudio del comportamiento de los programas legítimos del sistema, en busca de datos extraños que revelen la presencia de archivos no deseados: retrasos en la ejecución, irregularidades en el funcionamiento, consumo excesivo de memoria al ejecutarse...

3.- Protecciones

En ciberseguridad existen una serie de principios, denominados Leyes de Courtney, que conforman una especie de mandamientos no oficiales para los especialistas. Su elemento principal es la idea de que no debe protegerse una vulnerabilidad que resulta más cara de proteger que los daños que causaría un intruso al aprovecharse de ella. Esto no es más que puro sentido común, de la misma forma que no arreglamos la avería de un televisor cuando nos resulta más caro que comprar uno nuevo. Sin embargo, de esta idea se desprenden dos premisas -a las que los informáticos llaman corolarios- que convendría tener en cuenta en aventuras relacionadas con la ciberseguridad:

- Primer corolario: la seguridad perfecta tiene un coste infinito, puesto que siempre hay más medidas que pueden añadirse.

- Segundo corolario: Dado su coste infinito, la seguridad perfecta es inalcanzable, pues siempre excederá el valor de lo protegido. Eso significa que, en ciberseguridad, no existe el riesgo cero.

Tus jugadores deberán aprender a vivir con ello: por mucho cuidado que pongan en proteger sus sistemas, siempre existe la posibilidad de que sufran un ataque exitoso. No obstante, tienen varios elementos, protecciones y trampas con los que pueden reducir esos riesgos lo más cerca de cero que les permitan sus recursos. Aquí tienes una pequeña lista, para que no te falten ideas que incorporar a tus aventuras.

a) *Honey Pot*

En el argot de la ciberseguridad, un *honey pot* es una trampa destinada a reunir información sobre un intruso y a evitar que cause daño.

El atacante accede a una parte compartimentada del sistema que ataca, creyendo haber accedido al sistema propiamente dicho, pero solo se encuentra en una suerte de simulación preparada por los defensores. En ese espacio virtual acotado, el intruso realizará a cabo sus acciones, creyendo que no ha sido detectado y que está operando con libertad.

De esta forma, la seguridad consigue dos objetivos: el atacante no puede causar daño al sistema, aunque cree que sí lo está haciendo; y, por otra parte, la seguridad puede estudiar al intruso -qué pretende, que técnicas utiliza- y reunir información que permita su localización o su identificación.

Puedes pedir una tirada de Inteligencia a los personajes con la Especialidad Informática que deseen crear un *honey pot* para un sistema cibernético, pero en este caso, la Especialidad solo les permitirá efectuar la tirada, sin recibir una bonificación en ella. Solo en el caso de tener una Especialidad más concreta -por ejemplo, Ciberseguridad- se podrá recibir la bonificación de +2.

Cuando el PJ sea el agresor, lo lógico será pedirle una tirada equivalente para ver si se da cuenta de que se encuentra en un *honey pot*. La dificultad de la tirada debería variar según la habilidad del equipo que creó la trampa. Utiliza las Tablas de Incertidumbre de *Karma*, para que tus jugadores no conozcan el resultado de la tirada.

b) Sandbox

El sandbox, o cajón de arena, es un término que hace referencia a un tipo de defensa consistente en crear barreras que impiden a determinados programas alterar contenidos del sistema, de forma que no pueden ser utilizados de forma maliciosa. El programa puede utilizarse con normalidad dentro de los límites establecidos -el “cajón de arena”-, pero sin alterar el sistema; de la misma forma en que un niño puede jugar dentro de un cajón de arena, sin peligro de que se haga daño o de que cause un entuerto en otra parte del jardín.

Cuando se realiza una incursión en un sistema protegido con un sandbox, el atacante debe intentar superarlo con una tirada. Aunque pueda resultar parecido a un *honey pot*, el sandbox no pretende engañar al atacante, pues este sabe que se encuentra en uno. Por ello, la dificultad para crear un sandbox es mucho menor.

Una interesante cuestión de juego es qué hacer si un personaje falla su tirada para tratar de superar el sandbox durante una penetración. Sería posible que lo intentara una y otra vez hasta conseguirlo, pero, al tiempo, resultaría poco realista. Una solución es permitir un número máximo de intentos, estableciendo que, si el PJ no ha conseguido el Éxito una vez agotados, la barrera es demasiado buena para sus capacidades y no conseguirá superarla. Es conveniente que cada nuevo intento suponga un coste para el personaje, de modo que no dé igual superarlo a la primera que al tercer intento. Para ello, juega con el Karma, la Felicidad y los Estados Temporales.

c) Intrusion Prevention System (IPS)

El Sistema de Prevención de Intrusos es un programa defensivo destinado a localizar y contener cualquier intento de penetrar ilegítimamente en un sistema informático.

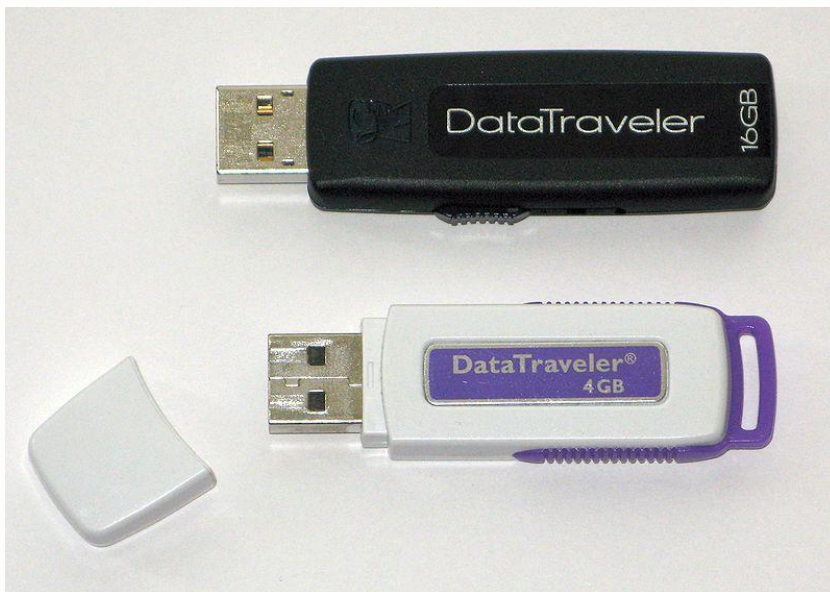
Cuando un personaje trate de vulnerar un sistema que cuente con IPS, deberá superar mediante tiradas la capacidad del programa para contener su penetración.

Si, además de IPS, existe un especialista que está intentando contener al atacante, el IPS debe otorgar una bonificación a las acciones de este especialista o un penalizador a las del atacante, según cuál de los dos sea el PJ.

d) Token, o mochila

El token, al que a veces se denomina “mochila” en el mundo hispanohablante es un dispositivo externo -por ejemplo, un USB- que debe conectarse físicamente a un equipo informático si se quiere que este pueda utilizar determinadas aplicaciones o llevar a cabo ciertas acciones.

Se dispone, así, de un nivel de seguridad adicional, puesto que alguien que acceda a través de la red al equipo no podrá ejecutar esas funcionalidades a menos que coloque físicamente el token en el equipo.



Como es lógico, el token se inserta solo durante el tiempo necesario para que el usuario legítimo ejecute el programa o la acción, y después se retira de nuevo.

e) Elementos de autenticación

Solo un usuario legítimo puede acceder a un equipo o realizar determinadas acciones en él, pero para poder diferenciar al usuario legítimo del atacante ilegítimo necesitamos algo. Ese algo son los elementos de autenticación, que podemos dividir en tres tipos:

- Algo que el usuario legítimo sabe: una contraseña o la respuesta a una pregunta personal.

- Algo que el usuario legítimo tiene: una llave, un token u otro elemento de naturaleza física que debe mostrarse o insertarse en el equipo.

- Algo que el usuario legítimo es: es decir, un parámetro biométrico inalterable y que diferencia al usuario de todos los demás seres humanos. Los más habituales son la huella dactilar, la voz o el patrón de la retina.

Los sistemas mejor protegidos no se conforman con uno solo de estos métodos, y combinan varios: una contraseña y la huella dactilar, una pregunta personal y un token físico... A esto se le llama autenticación multifactor.

f) Bastión

Imagina una red de ordenadores. No resulta difícil. Ahora imagina que esa red de ordenadores se conecta a Internet a través de un único punto de acceso. Por ejemplo, un único equipo: todos los ordenadores de la oficina conectan con el ordenador X, y este conecta a Internet, de manera que toda la información que de la oficina salga a Internet o de Internet entre a los equipos de la oficina pasa por ese ordenador X. Imagina, por tanto, que ese ordenador es la puerta por la que se entra y se sale a una ciudad. Imagina ahora qué harías con esa puerta... En efecto: protegerla. Hacer que cualquiera que quisiera introducir algo o sacar algo a través de ella tuviera que superar todo tipo de defensas, muros, trampas, fosos...

Lo que has imaginado, en términos de ciberseguridad, se denomina bastión: un equipo ultra protegido ejerce como “puerta” que tiene que atravesar todo el tráfico que entra o sale a Internet procedente del resto de la red.

Atravesar un bastión debería ser una acción, cuando menos, Difícil. Puedes hacer que tenga también trampas, como *honey pots*, o dispositivos del tipo IPS, así como cualquier otra cosa que el responsable de seguridad hubiera tenido tiempo y capacidad para implementar.

g) Bóveda electrónica

Las bóvedas electrónicas son espacios de almacenamiento virtual en el ciberespacio, altamente protegidos, que permiten a sus clientes guardar en ellas copias de seguridad de sus sistemas y sus redes, de forma que el cliente se ahorra los costes de tener que implementar él mismo la arquitectura de seguridad y almacenamiento, y en su lugar paga una cantidad por el servicio a la empresa propietaria de la bóveda, enviando cada cierto tiempo la copia de seguridad de sus archivos.

Desde el punto de vista de juego, los personajes podrían tener dos motivos para realizar una incursión contra una bóveda electrónica: destruir todas las copias existentes de una información o robar una información almacenada en la bóveda.

Un ataque a una bóveda debe ser algo difícil de llevar a cabo con éxito, puesto que la esencia de las bóvedas es garantizar la protección de la información que custodian.

h) Esquema umbral

El esquema umbral es un modelo de división de datos destinado a dificultar el acceso a los mismos a quien no está autorizado. Esto se hace dividiendo la información entre varios actores legítimos y creando un protocolo de seguridad que requiere reunir un número predeterminado de fragmentos para acceder a la información completa.

Ejemplo: los personajes reciben el encargo de proteger una valiosa secuenciación genética que tiene gran importancia para la empresa farmacéutica que los ha contratado. Deciden crear un esquema umbral, por lo que dividen la información en cinco fragmentos, cada uno de los cuales es custodiado por un ejecutivo diferente en un ordenador diferente, y establecen que son necesarios tres fragmentos para poder acceder a la información completa. De este modo, un intruso que quiera reunir la secuencia genética tendrá que acceder al menos a tres de los bloques de información para llegar hasta la secuencia completa.

Quizá esto te ayude a entender mejor cómo funciona un esquema umbral: piensa en cada uno de los fragmentos en que se divide la información no como información, sino como una llave: si reúnes tres llaves, puedes ver todo el conjunto; pero una de las llaves por sí sola no te da ninguna información: no te permite abrir la puerta. Ni siquiera mirar por la mirilla.

i) Código de Autenticación de mensajes

Este recurso de seguridad lo has visto en un millar de películas de espías: para que quien recibe un mensaje sepa a ciencia cierta que dicho mensaje es auténtico, el texto debe contener una palabra concreta.

En realidad, esto se puede reducir a un único carácter, que puede ser un número, un signo, o algo más complejo y preciso, como que el carácter tenga que ocupar una posición exacta dentro del mensaje.

Igual que un código de autenticación se incluye en un mensaje entre receptores humanos -como una carta, una llamada telefónica, un telegrama, etc.-, también puede ser incluido como parte de un código de programación, de tal manera que cualquier intento de simular una conexión auténtica mediante un malware debe replicar el código de autenticación del programa al que suplanta o el equipo receptor detectará que está siendo víctima de un ataque.

En términos de juego, esto supone que debes pedir al PJ que está enviando el mensaje falso una tirada para ver si se da cuenta de que existe un código de autenticación en la comunicación que intenta imitar. Un Éxito Parcial, en este caso, podría suponer que el PJ se da cuenta de que hay un código de autenticación, pero no logra descubrir con exactitud cuál es.

CLASS OF SERVICE DESIRED	
Fast Day Message	<input checked="" type="checkbox"/>
Day Letter	<input type="checkbox"/>
Night Message	<input type="checkbox"/>
Night Letter	<input type="checkbox"/>

Patrons should mark an X opposite the class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Rate No.	15
Class	5500
Time Filed	

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 29 1917

GERMAN LEGATION
MEXICO CITY

130	13042	13401	8501	115	3528	416	17214	6491	11310
18147	18222	21580	10247	11518	23677	13605	3494	14936	
98092	5905	11311	10392	10371	0302	21290	5161	39695	
23571	17504	11269	18276	18101	0317	0228	17694	4473	
22284	22200	19452	21589	67893	5569	13918	8958	12137	
1333	4725	4458	5905	17166	13851	4458	17149	14471	6706
13850	12224	6929	14991	7382	15857	67893	14218	36477	
5870	17553	67893	5870	5454	16102	15217	22801	17138	
21001	17388	7446	23638	18222	6719	14331	15021	23845	
3158	23552	22096	21604	4797	9497	22464	20855	4377	
23610	18140	22260	5905	13347	20420	39689	13732	20667	
6929	5275	18507	52262	1340	22049	13339	11265	22295	
10439	14814	4178	6992	8784	7632	7357	6926	52262	11267
21100	21272	9346	9559	22464	15874	18502	18500	15857	
2188	5376	7381	98092	16127	13486	9350	9220	76036	14219
5144	2831	17320	11347	17142	11264	7667	7762	15099	9110
10482	97556	3569	3670						

BEPNSTOFFF.

Charge German Embassy.

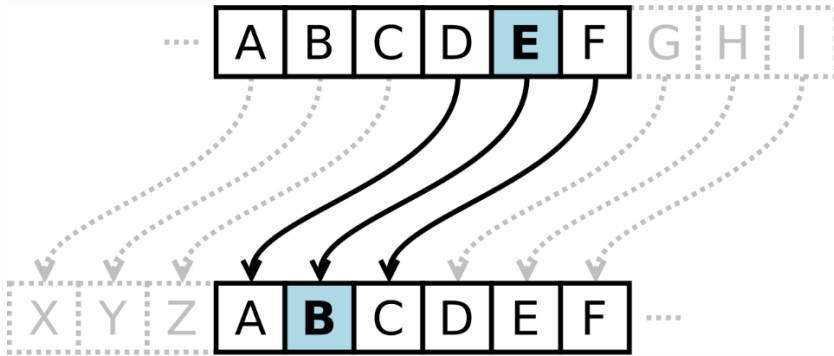
-El Telegrama Zimmerman, cuya interceptación y decodificación propicio la entrada de Estados Unidos en la Primera Guerra Mundial-

j) Algoritmo de confusión

Se trata de un tipo de algoritmo que, cuando se codifica un texto, inserta una serie de caracteres que no tienen nada que ver ni con el mensaje codificado ni con el código utilizado, de forma que dificulta su descifrado no autorizado al llenarlo de elementos que, en realidad, no son más que ruido blanco, no significan nada y no generan más que confusión dentro del texto, impidiendo su descifrado en base al estudio estadístico de los símbolos que aparecen.

Estos algoritmos se desarrollaron para inutilizar sistemas de descifrado basados en la frecuencia estadística con la que cada letra se utiliza en un idioma. Así, en inglés la letra que más se repite es la “e”, mientras que en castellano es la “a”. En base a ese dato, el descifrado se inicia partiendo de la suposición de que el signo más repetido tenía más posibilidades de ser la “e”, en el caso inglés, que, por ejemplo, la “x”, la letra menos utilizada, brindando un punto de partida a quien deseaba romper el código.

Si un PJ añade un algoritmo de confusión a sus códigos, estos serán más difíciles de romper; lo mismo ocurrirá si es el PJ quien trata de descifrar un código que incluye un algoritmo de confusión: debería recibir un modificador de -1 a su tirada, puesto que inutiliza algunos de los métodos de descifrado más comunes.



- Sistema de cifrado de Julio César, en el que cada letra es sustituida por otra de forma correlativa a su posición en el alfabeto-

k) Cortafuegos o *Firewall*

Elemento de seguridad de bajo nivel, consistente en una suerte de muro virtual que impide el acceso a usuarios o programas no autorizados. En sus versiones más avanzadas estaríamos hablando de los IPS.

Quando un cortafuegos está diseñado para no ser percibido por los intrusos recibe la denominación de “cortafuegos transparente”, y el atacante solo se da cuenta de que existe cuando “choca” contra él, viendo su incursión bloqueada.

1) Defensa en profundidad

Este concepto proviene de la terminología militar, y hace referencia a aquellas medidas de seguridad que se disponen en diferentes capas o líneas de defensa, de modo que el atacante tiene que penetrarlas de forma sucesiva para acceder al sistema. Así, un solo éxito no es suficiente, pues superadas las defensas exteriores, el intruso se enfrenta a un nuevo anillo, y así tantas veces como profundidad se haya dado al sistema defensivo.

En términos de juego, las defensas en profundidad pueden ser un gran desafío para los PJ, ya que, con frecuencia, una incursión se realiza contrarreloj y cada nueva línea de defensas supondrá una nueva tirada, con el riesgo que conlleva. Quizá la segunda línea defensiva no sea más difícil de superar que la primera, pero el mero hecho de tener que hacerlo ya aumenta las posibilidades de que el atacante fracase...

En todo caso, no recomendamos que cuando enfrentes a tus personajes a defensas en profundidad esto les requiera un número alto de líneas sucesivas. Lo normal deberían ser dos anillos de protección, y solo en casos excepcionales podría llegarse a los tres. Números más altos pueden generar frustración, la sensación de que se les va a hacer tirar hasta que fallen y el aburrimiento de repetir una y otra vez la misma acción.

m) Efecto Avalancha

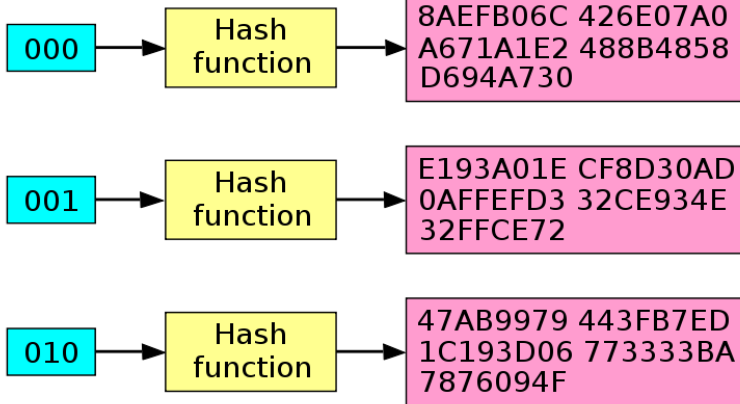
El Efecto Avalancha se produce cuando el algoritmo que se utiliza para cifrar un mensaje hace que un cambio mínimo en el texto sin cifrar produzca una alteración desproporcionada en el mensaje cifrado.

Los códigos que tienen este tipo de algoritmos son mucho más difíciles de descifrar, por lo que, si el código que un personaje quiere romper tiene esta propiedad, añade un -1 a la dificultad de la acción.

Las medidas de seguridad de un código se deben acumular mecánicamente a la dificultad de la tirada para romperlo. Un código de Dificultad media (+0), que tuviera un algoritmo de Efecto Avalancha (-1), y además un algoritmo de confusión (-1), sería Muy Difícil (-2) de romper para un personaje.

Input

Hash sum



- Ejemplo de efecto avalancha-

CAPÍTULO VIII: GLOSARIO

- *Adware*: característica del malware que indica que el código añade publicidad en el ordenador infectado, comúnmente en su navegación por Internet, agregando *popups*, clicks maliciosos, cambiando el resultado cuando se hace uso de buscadores, etcétera.

- Amenazas Persistentes Avanzadas (APT) son ataques que se guardan en el disco duro de los dispositivos del objetivo, de modo que son persistentes al reinicio del dispositivo.

- Amenazas Volátiles Avanzadas (AVT): ataques que se guardan en la memoria RAM de los dispositivos del objetivo, desapareciendo en el momento en el que se reinician. Son empleadas generalmente en labores de espionaje.

- Análisis forense: metodología que analiza, a posteriori, los ataques cibernéticos, tratando de reconstruir su curso y valorar los daños causados.

- Análisis heurístico: análisis para localizar malware basado en el estudio del comportamiento de los programas, buscando irregularidades que pudieran delatar su presencia.

- Ataque de diccionario: ataque de fuerza bruta que trata de descifrar una contraseña probando con todas las palabras que existen en la lengua en que se supone que está escrita la clave.

- Ataque de fuerza bruta: ataque consistente en tratar de descifrar una contraseña probando todas las combinaciones posibles.

- Ataques de intermediario, o Man in the Middle (MitM). Es la irrupción dentro del canal de comunicación entre el cliente y el servidor para interceptar el tráfico que se realiza entre ambos.

- Ataques dirigidos: aquellos que se dirigen contra un objetivo individualizado.

- Autenticidad: características de la información que permite identificar la fuente de la que emana, permitiendo determinar quién es su autor.

- Autenticación multifactor: cuando las medidas de seguridad de un sistema exigen al usuario legítimo que demuestre su identidad mediante la combinación de dos o más métodos: claves, contraseñas, preguntas, tokens, huellas, voz...

- *Backdoor*: característica del malware que establece un acceso en el equipo infectado, permitiendo su control en remoto.

- *Banker*: sub-característica del *spyware* en la que el malware roba las credenciales bancarias de los afectados para hacerse con el control de sus cuentas, recopilando información acerca de sus conexiones bancarias y, en muchos casos, modificando su navegación con la finalidad de engañarles.

- Bastión: equipo que ejerce de único acceso a Internet de un sistema o red y que se encuentra protegido al máximo nivel, como si se tratara de la puerta de entrada en una ciudad amurallada, analogía de la que toma su nombre.

- Basuring: técnica de penetración consistente en acceder a la papelera de reciclaje de un equipo informático y a otros elementos borrados para reunir información sobre el sistema, los usuarios, etc.

- Bomba lógica: malware que, una vez instalado, permanece inactivo hasta que un evento preprogramado lo activa.

- Botnet: red de ordenadores -denominados, en argot, zombisque, tras ser infectados por malware, pasan a estar controlados por otro equipo, normalmente sin que el dueño o usuario del ordenador infectado sea consciente de ello.

- Bóveda de seguridad: espacio virtual en el que se custodian copias de seguridad de sistemas o redes.

- Ciberactivismo: forma pacífica de protesta en la que se utilizan medios digitales para propagar un mensaje específico en torno a un problema social o político.

- Cibercrimen o ciberdelincuencia: actividad cibernética ilegal cuyo fin es la consecución de un lucro económico.

- Ciberespacio: espacio virtual donde, a partir de ciertos tipos de software, redes, tecnologías, dispositivos, etcétera, se crean y diseñan elementos que no existen en forma física, con los que se puede interactuar.

- Ciberguerra: actividad cibernética cuyo fin es la consecución de determinados objetivos políticos y en la que los atacantes son miembros de un organización estatal o supraestatal.

- Ciberseguridad: también denominada seguridad informática o seguridad de tecnologías de la información, es la disciplina encargada de la protección de la información contenida o transferida a través de la tecnología informática.

- Ciberterrorismo: delito cibernético cuyo fin es provocar miedo e inestabilidad, a fin de intimidar a un gobierno o sociedad para acceda a las metas políticas de los ciberterroristas.

- Clearnet o Red de Superficie: la parte de Internet fácilmente accesible para cualquier usuario desde cualquier navegador.

- Código de autenticación de mensajes: un carácter o conjunto de caracteres que debe aparecer en un mensaje para que el receptor pueda identificar con certeza al emisor.

- Contrainteligencia cibernética: aquellas técnicas con las que se engaña a los actores mediante la utilización de señuelos para que éstos crean que están perpetrando un ataque exitoso cuando en realidad están contribuyendo a la investigación.

- Cortafuegos: Elemento de seguridad consistente en una suerte de muro virtual que impide el acceso a usuarios o programas no autorizados. Cuando su diseño lo hace invisible para los atacantes se habla de “cortafuegos transparente”.

- Cracker: especialista en accesos no autorizados con el fin de causar daño en el uso, programa o equipo al que se acceder, por lo que su actividad siempre es ilegal.

- Dark Web o Internet Oscura: Es el 0,1% de la Deep Web, formada por el contenido que ha sido ocultado de forma deliberada y que solamente es accesible a través de las Darknets.

- Darknet: red a la que el usuario solo se puede introducir mediante herramientas y programas específicos que logran su anonimato, ocultando su identidad, geolocalización y actividad. Por ejemplo, TOR; I2P o Freenet.

- Deep Web o Internet Profunda: abarca alrededor del 90% Internet e incluye todas las páginas y sitios web a los que se accede mediante los buscadores tradicionales, páginas web que requieren registro previo y los servicios de correo electrónico.

- Defacement: ataque contra una web consistente en la alteración de la parte que es visible de forma pública.

- Defensa en profundidad: método de seguridad consistente en disponer de varias líneas de protección, de modo que, si un atacante supera la primera, tope con un segundo anillo de medidas defensivas.

- Denegación de servicio: ataque bastante común, que disminuye la capacidad de una red para prestar su servicio.

- Dirección IP: procede del inglés *Internet Protocol* y es un número que se asigna a cada usuario al conectarse a la red, mediante el cual se le identifica, permitiendo obtener información sobre él (geolocalización, propietario, etcétera), pero son fáciles de alterar o enmascarar.

- Dominio: nombre que identifica de manera exclusiva a toda página o sitio web. Es la traducción de cada dirección IP a un nombre legible y memorizable.

- *Downloader* o *Loader*: característica del malware que indica que el código descarga aplicaciones que instala o ejecuta en el equipo de la víctima sin que se dé cuenta, añadiendo funcionalidades maliciosas.

- Drive-by: malware que se instala en un equipo cuando visita una página web infectada, sin necesidad de realizar ninguna otra interacción.

- Efecto avalancha: propiedad de los códigos en los que un cambio mínimo del mensaje original genera cambios muy grandes en el mensaje cifrado, dificultando el que pueda ser descifrado.

- Envenenar el motor de búsqueda: ataque consistente en “contaminar” el buscador de Internet que usa un equipo, de modo que los resultados de las búsquedas envíen al usuario a las páginas que interesan al atacante, muchas veces infectadas con malware.

- Esquema umbral: modelo de seguridad que divide una información en bloques separados, de forma que cada uno por sí mismo no permite acceder a ella y son necesarios varios para tener disponible la información.

- Exploit: programa o código cuya finalidad es aprovechar o explotar una vulnerabilidad concreta.

- *FakeAV*: característica del malware que indica que el código se hace pasar por un antivirus.

- *Form grabber*: sub-característica del *spyware* en la que el malware roba la información que los navegadores remiten al servidor cuando el usuario completa un formulario.

- Gusano o *Worm*: característica del malware que indica que el código se replica a través de la red en distintos ordenadores haciendo uso de vulnerabilidades, credenciales robadas o débiles, etc.

- Hactivismo: vertiente del ciberactivismo en la que se emprenden acciones ilegales en la red para alcanzar los mismos objetivos que en el ciberactivismo pacífico. El término proviene de la unión de los términos “*hacking*” y “activismo”.

- Hash: algoritmo matemático que permite identificar un fichero digital de forma inequívoca. Cada hash es único, de modo que, si se modifica una parte del fichero, se genera otro hash que lo diferencia del original. Como cada hash es único, resulta sencillo para los investigadores comprobar, mediante su análisis, si un fichero es legítimo o si se encuentra modificado por malware.

- *Honey pot*: trampa defensiva en la que un intruso es desviado a una sección compartimentada del sistema atacado sin que se dé cuenta, impidiendo que cause daño y pudiendo observar sus objetivos, métodos, etc.

- Indicadores de compromiso: señales de que un equipo ha sido comprometido mediante un ataque.

- Ingeniería social: técnicas que recurren a la manipulación psicológica y al engaño de la víctima, existiendo un componente de interacción humana, y haciendo que la propia víctima sea quien actúa sobre su equipo.

- *Intrusion Prevention System (IPS)*: programa defensivo destinado a localizar y contener cualquier intento de penetrar ilegítimamente en un sistema informático.

- Irrenunciabilidad o no repudio: característica de la información que impide que el emisor pueda negar el envío de la comunicación (no repudio en origen) y que el emisor pueda negar la recepción del mensaje (no repudio en destino).

- *Keylogger*: sub-característica del *spyware* en la que el malware registra las pulsaciones de teclado.

- Kilos: buscador de contenidos para la Dark Web.

- **Malware:** cualquier tipo de software cuya finalidad es comprometer un dispositivo o infiltrarse en él sin la autorización y el conocimiento de su propietario. Es la unión de las palabras “*malicious software*”: código dañino o software malicioso.

- **Mineros:** característica del malware que indica que el código se instala en el ordenador para llevar a cabo un proceso de minado mediante el cual consume la capacidad de procesamiento del sistema, con la finalidad de producir criptomonedas.

- **Phishing:** estafa cibernética basada en la ingeniería social, que consiste en la emisión de una comunicación electrónica aparentemente oficial a la víctima, en la que el atacante finge ser una entidad legítima o de confianza que solicita al usuario realizar alguna acción.

- **Pharming:** ataque consistente en reescribir la dirección IP que el usuario legítimo quiere visitar, redirigiéndole a una página falsa donde introduce sus claves creyendo que está en la web que quería visitar originalmente.

- **Ransomware:** característica del malware que indica que el código cifra parte del sistema, bloqueando el acceso a los usuarios a la información y/o servicios que este ofrece, pidiendo un rescate por su recuperación.

Dear Customer:

It is time to pay for your software lease from PC Cyborg Corporation. Complete the INVOICE and attach payment for the lease option of your choice. If you don't use the printed INVOICE, then be sure to refer to the important reference numbers below in all correspondence. In return you will receive:

- a renewal software package with easy-to-follow, complete instructions;
- an automatic, self-installing diskette that anyone can apply in minutes.

Important reference numbers: A5599796-2695577-

The price of 365 user applications is US\$189. The price of a lease for the lifetime of your hard disk is US\$378. You must enclose a bankers draft, cashier's check or international money order payable to PC CYBORG CORPORATION for the full amount of \$189 or \$378 with your order. Include your name, company, address, city, state, country, zip or postal code. Mail your order to PC Cyborg Corporation, P.O. Box 87-17-44, Panama 7, Panama.

Press ENTER to continue

-Mensaje del AIDS DOS para que la víctima pague al atacante-

- *Rootkit*: técnica que permite al malware ocultarse en el sistema, modificando ciertos archivos en el núcleo, lo que hace muy complicada su detección.

- *Sandbox*: elemento de ciberseguridad que permite funcionar a los programas a los que afecta, al tiempo que impide que puedan alterar el equipo.

- *Scareware*: característica del malware que indica que el código tiene la intención de asustar a la víctima, con ánimo de lograr un beneficio económico de sus acciones en consecuencia.

- *Script Kiddie*: término despectivo que hace referencia a quien no es capaz de crear sus propios códigos y, por tanto, se limita a utilizar programas creados por otros.

- *Secuestro de sesión*: ataque a un entorno protegido con clave, en el que el intruso toma temporalmente el control de una sesión que ha sido iniciada por un usuario legítimo.

- *Spyware* o *Stealer*: característica del malware que indica que el código tiene la intencionalidad de espiar las acciones del usuario.

- Técnicas avanzadas de evasión: conjunto de métodos altamente especializados con las que un atacante trata de ocultar el rastro de sus acciones.

- The Hidden Wiki: Índice o directorio de páginas con extensión .onion a las que se puede acceder a través de TOR.

- Token, o mochila: dispositivo externo que debe conectarse a un equipo para que este pueda ejecutar determinados programas o realizar ciertas acciones.

- TOR: Darknet de la Internet Oscura, que busca garantizar el anonimato de sus usuarios.

- Trazabilidad: característica de la información que permite atribuir una actividad o actuación, a un determinado usuario o entidad.

- Troyano o *Trojan*: característica del malware que simula constituir un programa legítimo, para que el usuario lo instale y ejecute, llevando en su interior la carga maliciosa. Con el tiempo, se utilizó como un término genérico para describir cualquier malware que proporciona al atacante control del equipo y, a día de hoy, se usa para definir cualquier malware que se instala en el ordenador.

- Virus: característica del malware que indica que, independientemente de su objetivo, el código se replica modificando ficheros del sistema, pasando desapercibido e infectando a otros sistemas, si copian esos archivos.

- Vulnerabilidad: todas aquellas debilidades o fallos que se producen en los sistemas informáticos.

- War chalking: marcar con tiza el exterior de una zona donde hay una red inalámbrica desprotegida, para que otros puedan usarla.

- Watering Hole: ataque consistente en infectar una web frecuentada por el objetivo, a fin de que este resulte “contaminado” durante sus visitas.

- Whaling: ataque de phishing en el que el blanco es un individuo o un grupo de individuos concreto y, por lo general, de alto nivel dentro de la estructura atacada.

- Zombi: cada uno de los ordenadores infectados en una botnet.

LICENCIA DE USO

Queda permitida la reproducción y distribución no comercial de este material, siempre que se realice respetando la integridad de la obra, los contenidos se pongan a disposición del público de forma libre y gratuita y se haga constar la autoría del material original.

Los usos comerciales, así como cualquier otro que se aparte del contenido del párrafo anterior en forma o fondo, quedan reservados a los propietarios de los derechos o a en quienes estos hagan cesión de los mismos.

Estaremos encantados de conocer vuestras sugerencias, ideas, creaciones: escenarios de campaña, módulos, aventuras... Cualquier cosa que queráis compartir con nosotros respecto de Karma podéis hacérselo llegar a la dirección Karmajuegoderol@gmail.com.

Esta licencia se aplica a todo el material contenido en la presente publicación, con excepción de la siguientes imágenes:

- Código de barras de Wikipedia: Dominio público.
https://es.wikipedia.org/wiki/Trazabilidad#/media/Archivo:Barcode_d_iagram.svg, consultada el 21 de enero de 2021.

- Logo de The Hidden Wiki: Dominio público
https://en.wikipedia.org/wiki/The_Hidden_Wiki#/media/File:The_Hidden_Wiki_logo.png, consultada el 21 de enero de 2021.

- Logo utilizado por el colectivo Anonymous: dominio público, [https://en.wikipedia.org/wiki/Anonymous_\(group\)#/media/File:Anonymous_emblem.svg](https://en.wikipedia.org/wiki/Anonymous_(group)#/media/File:Anonymous_emblem.svg), consultada el 21 de enero de 2021.

- Firmantes del convenio de Budapest: dominio público, https://en.wikipedia.org/wiki/Convention_on_Cybercrime#/media/File:Ratified_Convention_on_Cybercrime.svg, consultada el 21 de enero de 2021.

- Centro de ciberseguridad de la US Navy: dominio público, https://en.wikipedia.org/wiki/Cybercrime#/media/File:U.S._Navy_Cyber_Defense_Operations_Command_monitor.jpg, consultada el 21 de enero de 2021.

- Web bloqueada por el FBI por un ataque DDoS: dominio público, https://en.wikipedia.org/wiki/Denial-of-service_attack#/media/File:FBI_DDoS_domain_seized.png, consultada el 21 de enero de 2021.

- Mapeado de ARPANET: Dominio público, https://en.wikipedia.org/wiki/ARPANET#/media/File:Arpanet_logical_map_march_1977.png, consultada el 21 de enero de 2021.

- Código del gusano Blaster: Dominio público, https://en.wikipedia.org/wiki/Computer_virus#/media/File:Virus_Blaster.jpg, consultada el 21 de enero de 2021.

-Mensaje del AIDS DOS para que la víctima pagara al atacante: [https://es.wikipedia.org/wiki/AIDS_\(troyano\)#/media/Archivo:AIDS_DOS_Trojan.png](https://es.wikipedia.org/wiki/AIDS_(troyano)#/media/Archivo:AIDS_DOS_Trojan.png), consultada el 21 de enero de 2021.

- Memorias USB: dominio público: https://ast.wikipedia.org/wiki/Malware#/media/Ficheru:Kingston_US_B_Memory.jpg, consultada el 21 de enero de 2021.

- Máquina Enigma: dominio público,
<https://en.wikipedia.org/wiki/Cryptography#/media/File:Enigma.jpg>,
consultada el 21 de enero de 2021.

- Cuartel general de la NSA, Fort Meade, Maryland: Dominio público,
https://en.wikipedia.org/wiki/Cryptography#/media/File:National_Security_Agency_headquarters,_Fort_Meade,_Maryland.jpg, consultada el 21 de enero de 2021.

- Sistema de cifrado de Julio César: dominio público,
https://en.wikipedia.org/wiki/Caesar_cipher#/media/File:Caesar_cipher_left_shift_of_3.svg, consultada el 21 de enero de 2021.

- Hombre con gafas de realidad virtual: dominio público,
https://es.wikipedia.org/wiki/Ciberespacio#/media/Archivo:Realite_virtuelle.jpg, consultada el 21 de enero de 2021.

- Troyano Nuclear Rat: Dominio público,
[https://es.wikipedia.org/wiki/Troyano_\(inform%C3%A1tica\)#/media/Archivo:Nuclear_rat.png](https://es.wikipedia.org/wiki/Troyano_(inform%C3%A1tica)#/media/Archivo:Nuclear_rat.png), consultada el 21 de enero de 2021.

- Cartel de “se busca” por el FBI de un presunto miembro de Lazarus: Dominio público,
https://es.wikipedia.org/wiki/Lazarus_Group#/media/Archivo:Cartel_de_la_orden_de_captura_de_Park_Jin_Hyok.png, consultada el 21 de enero de 2021.

- Miembros del Grupo de Trabajo para la Alianza Estratégica contra el Cibercrimen: Dominio público:
https://es.wikipedia.org/wiki/Archivo:Saccwg_500_031708.jpg, consultada el 21 de enero de 2021.

- Imagen en pantalla de la primera versión de Petya: dominio público,

[https://en.wikipedia.org/wiki/Petya_\(malware\)#/media/File:2017_Petya_cyberattack_screenshot.jpg](https://en.wikipedia.org/wiki/Petya_(malware)#/media/File:2017_Petya_cyberattack_screenshot.jpg), consultada el 21 de enero de 2021.

- Evolución del phishing entre 2004 y 2005: Dominio público, https://es.wikipedia.org/wiki/Phishing#/media/Archivo:Phishing_chart_Oct_2004_to_June_2005.svg, consultada el 21 de enero de 2021.

-El Telegrama Zimmerman: Dominio público, https://en.wikipedia.org/wiki/Ciphertext#/media/File:Zimmermann_Telegram.jpeg, consultada el 21 de enero de 2021.

- Logo de Bitcoin: Dominio público: https://es.wikipedia.org/wiki/Internet_profunda#/media/Archivo:Bitcoin_logo.svg, consultada el 21 de enero de 2021.