Capítulo 4. El Ransomware y otros delitos relacionados.

1. EN RELACIÓN CON LOS DERECHOS FUNDAMENTALES.

- VULNERACIÓN DEL DERECHO FUNDAMENTAL A LA INTIMIDAD, HONOR Y PROPIA IMAGEN.

2. EN RELACIÓN CON LOS DELITOS PATRIMONIALES.

- VULNERACIÓN DELITO PROPIEDAD Y ESTAFA Y SU COMPARACIÓN.

3. RELACIÓN CON OTROS TIPOS DE DELITOS SEGÚN LA LEGISLACIÓN ESPAÑOLA.

- *ACCESO E INTERCEPTACIÓN ILÍCITA.*
- *INTERFERENCIA EN LOS DATOS Y EN EL SISTEMA.*
- *FALSIFICACIÓN INFORMÁTICA.*
- *FRAUDE INFORMÁTICO.*
- *DELITOS SEXUALES.*
- *CONTRA LA PROPIEDAD INDUSTRIAL E INTELECTUAL.*
- *CONTRA EL HONOR.*
- *DELITOS CONTRA LA SALUD PÚBLICA.*
- *AMENAZAS Y COACCIONES.*

1. En relación con los derechos fundamentales.

Vulneración de los derechos fundamentales a la intimidad, honor y propia imagen.

Los autores Alfredo García López[38], José Cuervo Díez[39] y Eva Muñoz Deiros[40] hacen referencia en sus publicaciones a la relación entre la vulneración de tales derechos y el ataque de Ransomware.

El derecho a la protección de datos es un derecho fundamental recogido en el artículo 18 de la Constitución Española, norma suprema de nuestro ordenamiento jurídico, y protege la intimidad y privacidad del ciudadano respecto al uso y vulneración de sus datos personales, es decir, de cualquier dato que identifique o pueda identificar a una persona física concreta, y también datos de carácter personal, por ejemplo, los vídeos y las fotografías.

La protección del derecho a la protección de los datos personales viene regulada, en vía civil y administrativa, por la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal y por el Reglamento que la desarrolla, el Real Decreto 1720/2007, de 21 de diciembre, además del Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), desarrollado anteriormente.

No obstante, el derecho a la protección de datos también está protegido en vía penal. Así, el apartado 2 del artículo 197 del Código Penal castiga a quien cometa delitos relativos a las infracciones del derecho fundamental a la protección de datos, concretamente:

Las mismas penas (penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses) se impondrán al que, sin estar autorizado, se apodere,

[38] (García López, A. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. , 2016)
[39] (Cuervo Díez, J. Delitos informáticos. Protección penal de la intimidad., 2014)
[40] (Muñoz Deiros, E. Delitos contra la protección de datos. , 2018)

utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

Por tanto, la protección de datos protege la intimidad y privacidad del ciudadano frente a una intromisión o vulneración de su derecho fundamental a la protección de datos.

Sin embargo, esta tipificación ha sido muy criticada por los autores ya que, según la doctrina, la regulación civil y administrativa sobre la protección de datos es suficiente, y la tipificación de la vulneración de este derecho como delito, complica la determinación de la conducta penal.

En conclusión, el derecho a la protección de datos está protegido en vía civil, administrativa y vía penal, pero ésta última vía, atendida la gravedad de sus consecuencias (penas privativas de libertad) solo es aplicable en última ratio, cuando no sea posible acudir o garantizar nuestro derecho a través de las vías civil y/o administrativa.

2. En relación con los delitos patrimoniales.

Vulneración del derecho a la propiedad y estafa[41].

En el capítulo VI del Código Penal, “de las defraudaciones”, en la sección 1, se tipifica el delito de estafa:

Artículo 248 1. “Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno”.

[41] (Oficina de Coordinación Cibernética. , 2018)

Esto hace referencia al engaño o manipulación que sufre la víctima mediante las técnicas de ingeniería social aplicadas por el ciberdelincuente para lograr así su objetivo.

2. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

c) Los que, utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

Este artículo especifica que el engaño y el lucro se obtienen a partir de la utilización de medios informáticos, programas informáticos y semejantes, para cometer el delito.

3. En relación con otros tipos de delitos según la legislación española[42].

A través del Observatorio español de delitos informáticos (oedi.es) se desarrollan otros tipos de delitos relacionados con el Ransomware.

Acceso e interceptación ilícita[43].

El Código Penal español, regula en los artículos 197 a 201 el descubrimiento y revelación de secretos, por un lado, y en los artículos 278 a 286 los delitos relativos al mercado y los consumidores.

[42] (Oficina de Coordinación Cibernética. , 2018)
[43] (Oficina de Coordinación Cibernética. , 2018)

Estamos ante un tipo de hecho de descubrimiento y revelación de secretos, de acceso ilegal informático y de otros accesos ilícitos que afectan al mercado y a los consumidores por las consecuencias negativas que tiene dicho acceso.

Las variables y los medios empleados son siempre Internet y los aparatos y programas informáticos, a través de la telefonía y las comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Interferencia en los datos y en el sistema.

El Código Penal español regula en los artículos 263 a 267 y 625.1 la interferencia en los datos y en el sistema y los daños informáticos.

Se trata de un tipo de hecho de daños derivados del ataque informático.

Las variables y los medios empleados son siempre Internet y los aparatos y programas informáticos, a través de la telefonía y las comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Falsificación Informática[44].

El Código Penal español regula el delito de falsificación informática en los artículos 388, 389, 399 bis, 400 y 401.

Se trata de un tipo de hecho de falsificación de moneda, sellos y efectos timbrados, fabricación y tenencia de útiles para falsificar y la usurpación del estado civil.

Las variables y los medios empleados son siempre Internet y los aparatos y programas informáticos, a través de la telefonía y las comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P,

[44] (Oficina de Coordinación Cibernética. , 2018)

páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Fraude Informático[45].

El Código Penal español regula en los artículos 248 a 251 y 623.4. el delito de fraude informático.

Se trata de un tipo de hecho relativo a la estafa bancaria, estafas con tarjetas de crédito, débito y cheques de viaje, así como otras estafas.

Las variables y los medios empleados son siempre Internet y los aparatos y programas informáticos, a través de la telefonía y las comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Delitos Sexuales[46].

El Código Penal español regula en los artículos 181, 183.1, 183.bis,184, 185, 186, 189 los diferentes delitos sexuales.

Los tipos de hecho son relativos al exhibicionismo, provocación sexual, acoso sexual, abuso sexual, corrupción de menores e incapacitados, pornografía infantil y el delito de contacto mediante tecnología con menores de 13 años con fines sexuales.

Las variables y los medios empleados son siempre Internet y los aparatos y programas informáticos, a través de la telefonía y las comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P,

[45] (Oficina de Coordinación Cibernética. , 2018)
[46] (Oficina de Coordinación Cibernética. , 2018)

páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Contra la propiedad industrial e intelectual[47].

El Código Penal español regula en los artículos 270 a 277 y 623.5 los delitos contra la propiedad intelectual y contra la propiedad industrial.

El tipo de hecho es el relativo a delitos contra la propiedad industrial y contra la propiedad intelectual.

Las variables y los medios empleados son siempre Internet y los aparatos y programas informáticos, a través de la telefonía y las comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Contra el Honor[48].

El Código Penal español regula en los artículos 205 a 210 y 620.2 los delitos contra el honor.

El tipo de hecho es relativo a los delitos de calumnias e injurias.

Las variables y los medios empleados son siempre Internet y los aparatos y programas informáticos, a través de la telefonía y las comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Delitos contra la salud pública[49].

[47] (Oficina de Coordinación Cibernética. , 2018)
[48] (Oficina de Coordinación Cibernética. , 2018)
[49] (Oficina de Coordinación Cibernética. , 2018)

El Código Penal español regula en los artículos 359 a 371 los delitos contra la salud pública.

El tipo de hecho es el relativo a los delitos de tráfico de drogas y otros delitos contra la salud pública.

Las variables y los medios empleados son siempre Internet y los aparatos y programas informáticos, a través de la telefonía y las comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

Amenazas y coacciones[50].

El Código Penal español regula en los artículos 169 a 172 y 620 los delitos de amenazas y coacciones.

El tipo de hecho es el relativo a los delitos de amenazas, amenazas a grupo étnico, cultural o religioso y las coacciones.

Las variables y los medios empleados son siempre Internet y los aparatos y programas informáticos, a través de la telefonía y las comunicaciones, intranet y otras redes, páginas de streaming, redes de archivos compartidos P2P, páginas de descargas directas, páginas de enlaces, blogs y correos electrónicos, redes sociales.

[50] (Oficina de Coordinación Cibernética. , 2018)

CAPÍTULO 5: Soluciones al problema.

1. CÓMO EVITARLO. PREVENCIÓN.

2. PROBLEMA DE EDUCACIÓN Y CONCIENCIACIÓN. LA VÍCTIMA NO DENUNCIA.

3. FORMACIÓN Y RECICLAJE DE LOS PERFILES DE RIESGO.

4. RECOMENDACIONES A SEGUIR EN CASO DE SER VÍCTIMAS DEL CIBER ATAQUE.

1. Cómo evitarlo. Prevención.

Existen diversas guías sobre cómo prevenir ser víctimas de este tipo de ciberataque, entre ellas, encontramos la Guía Eset[51] y la Guía de INCIBE[52].

Son diversas las medidas para evitar ser víctimas de un ciberataque de Ransomware y limitar sus daños, entre ellas encontramos medidas dirigidas a los sistemas, ya que deberían ser resistentes ante un ataque y poder recuperarse rápidamente cuando ocurre este ocurre, por ejemplo, si se tienen servicios públicos como un servidor Web, Correo, o alguna aplicación en Internet y está conectado a la red Interna, en la misma red de los usuarios de la empresa sin ninguna restricción esto es un grave error, ya que si cualquier servicio público es comprometido desde Internet o desde la red Interna que sería lo más probable, el atacante podrá ingresar a otros servicios de la red Interna sin ningún problema.

Para evitar casos así, es recomendable que los servicios públicos estén en una red independiente de la red interna como una DMZ para servicios públicos o una DMZ para Proveedores. Políticas de firewall tanto de entrada como de salida de tráfico. Registros de logging activado para identificar y revisar intentos de intrusión. Y aseguramiento del mismo servicio público a nivel del servidor como un hardening del servidor.

Otra medida muy importante para evitar ser víctimas de un ciberataque de Ransomware es la de realizar copia de seguridad, ya que contar con un sistema de recuperación de datos impide que una infección de ransomware pueda destruya los datos para siempre.

Es recomendable crear dos copias de seguridad, una para ser almacenada en la nube (se pueden usar servidores de servicio que realicen automáticamente copias de los archivos) y otra en un dispositivo físico, como un disco duro portátil, memoria USB, otro equipo portátil, etc.
Es importante desconectarlos del PC cuando se haya realizado la copia.

[51] (Guía Eset Ransomware 2017, s.f.)
[52] (INCIBE. Ransomware, una guía de aproximación para el empresario, s.f.)

Otras de las medidas básicas es usar un buen software antivirus para proteger el sistema del ransomware. No desactivar la detección mediante heurísticas ya que esto ayuda a capturar muestras de ransomware que aún no hayan sido detectadas formalmente.

Mantener el software del PC actualizado, y cuando el Sistema Operativo o aplicaciones se actualicen a una nueva versión hay que instalarlas.

No fiarse de nada, ya que cualquier cuenta puede estar comprometida y enlaces maliciosos pueden ser enviados desde cuentas en redes sociales de amigos, compañeros o desde juegos online.
No abrir nunca archivos adjuntos desde emails de alguien desconocido. Los cibercriminales a menudo distribuyen correos electrónicos falsos que simulan ser notificaciones legítimas remitidas desde servicios de almacenamiento en la nube, bancos, policía o agencias de recaudación de impuestos que incitan a pulsar enlaces maliciosos para instalar malware en los ordenadores y sistemas, esto se conoce como 'phishing'.

Activar la opción de mostrar las extensiones de los archivos en el menú de configuración de Windows. Esto hace mucho más fácil detectar archivos potencialmente maliciosos.
Mantenerse alejado de extensiones como ‘.exe’, ‘.vbs’ y ‘.scr’, ya que los estafadores pueden usar varias extensiones para camuflar un fichero malicioso como un video, una foto o un documento.

En caso de descubrir algún proceso sospechoso en el ordenador, hay desconectarlo inmediatamente de internet o de otras conexiones en red, como el WIFI de casa, para prevenir que la infección se propague.

Los técnicos deben velar por que los sistemas empleados se hallen actualizados de forma que al menos dispongan de la protección que el fabricante ha suministrado vía actualización de los parches o definición de virus.

Se deben observar reglas de uso adecuado de los medios para preservar las tres dimensiones de la seguridad de la información que son la confidencialidad,

la integridad y la disponibilidad de los datos, si el cumplimiento no es por parte de todos, estas dimensiones pueden verse afectadas. Confidencialidad: Exfiltración, publicación de información a quien no debiera verla. Integridad: Alteración, modificación de la información, caso de ransomware. Disponibilidad: Denegación, impedir el acceso a la información, caso de los Ataques que saturan los sistemas, ataques de Denegación de Servicio (DOS) o bien si son a gran escala Ataques Distribuidos de Denegación de Servicio (DDOS).

En las empresas y corporaciones.

1. No emplear los medios de la oficina para otra cosa que no sea el cometido del puesto de trabajo.
2. Comunicar un incidente cuando se produzca mediante los cauces establecidos y si estos no existen mediante cualquier medio al alcance.
3. No abrir correos sospechosos o que tengan algo que los haga sospechosos, como, por ejemplo: texto extraño o contenido poco habitual, el cuerpo del mensaje “pide dinero” o pide algo no habitual como que se realice un acceso a su web. Otro ejemplo, es un correo de publicidad con un ZIP anexo, oferta novedosa o mail del banco: “estamos actualizando la información debe acceder a su cuenta e introducir su número de cuenta”. Los bancos nunca piden el número de cuenta, lo único que piden son el identificador de acceso y la clave que debe ser oculta. Si un banco pide que le envíes la clave en texto, hay que llamar al banco.

4. No ejecutar programas que “aparecen” en la web tipo: “instale esto y le permitiremos bajar el archivo” o “su pc es vulnerable, escanéelo ahora con este programa”, “llame a este 908 para bajar…” ya que suele tratarse de malware.

En caso de que dicha prevención falle, se debe reaccionar:

[53] (INCIBE. Ransomware, una guía de aproximación para el empresario, s.f.)

Si se recibe un mail y al abrir el adjunto la pantalla parpadea o bien el adjunto de Office no se abre o bien se abre y el Excel/Word se cierra a continuación, es posible que haya sido infectado. En ese caso se debe avisar a los equipos de soporte.

Detener un ataque es muy difícil, así que la empresa debe tener procedimientos robustos de detección, supervisión y corrección, la capacidad de informar sobre todas las sospechas y agilidad a la hora de responder.

En los hogares y entornos no profesionales o corporativos.

Se vuelve a hacer hincapié en la prevención. Unificar la información personal en una carpeta (Mis Documentos, Mis Imágenes…), para facilitar la copia de seguridad, si se tiene la información dispersa en el disco duro hacer un Backpus será más complejo.
Es recomendable comprar un disco duro externo y hacer copia de los datos a este medio externo.
Establecer una rutina de actualización de la información, éstas acciones tienen que tener continuidad, tener un backup de hace 3 años puede que no me sirva de nada, por tanto, a la hora de establecer un proceso de copia debe establecerse una rutina de actualización, cada día, cada semana o cada mes.
Revisar que Windows Update o el sistema operativo utilizado esté al día, si no es así actualizar el equipo.
Y actualizar Antivirus/Malware en todos los equipos.

Es importante explicar a todos los usuarios del PC que no deben abrir correos sospechosos, ni deben ejecutar programas que aparecen en el web tipo “instale esto y le permitiremos bajar el archivo” o “su pc es vulnerable, escanéelo ahora con este programa”, suele ser malware. Usar un bloqueador de elementos emergentes en los navegadores. Usar UAC (Control de cuentas de usuario de Windows).

Si la prevención falla, se debe reaccionar de manera eficaz, si ve que la información ya no está disponible o bien los archivos cambian de nombre o bien el equipo se queda colgado, es posible que tenga un malware cifrando la

información. En ese caso se debe apagar el equipo y buscar asesoramiento para restaurar la información, evaluar hasta dónde ha llegado o bien probar la solución de la infección completa.
También se puede restaurar la información desde el punto de restauración anterior y revisar que la información se halle actualizada.
Si ya han infectado del todo y al abrir cualquier archivo aparece el mensaje de aviso del Ransomware para proceder al pago, se debe en lugar en pagar, buscar soluciones ya existentes en www.nomoreransom.org, web que más adelante se desarrollará.

2. Problema de educación y concienciación. La víctima no denuncia.

En España, el número de denuncias de Ransomware es inferior al del número de víctimas (500.000 es el número estimado de víctimas del Ransomware Cryptolocker), lo que quiere decir que la gente no denuncia, siendo fundamental para poder perseguir el delito policial y judicialmente.

Se puede denunciar este tipo de ataques por teléfono, por internet o en comisaría, en las instancias de la guardia civil o de la policía nacional, los cuales cuentan con unidades especializadas en delitos informáticos y fraudes a través de internet. Además de otros organismos internacionales y supranacionales, como Europol, Interpol, etc.

Los usuarios vulnerables son los que están desinformados, aquellos que no están alertas si reciben un correo falso, que creen que el ransomware es un tema de películas o que los incidentes de seguridad ocurren únicamente en gobiernos y grandes corporaciones multinacionales.
La mayoría de las infecciones de ransomware requieren, de la intervención del usuario: ya sea para descargar un archivo, ingresar a un link malicioso, abrir un documento o realizar el pago creyendo algún engaño.
El factor de ingeniería social es clave para el éxito de la infección.

Por lo tanto, otro punto importante en la prevención es la educación y concientización de los usuarios. Estar informado sobre cómo actúan las

amenazas, cuáles son los engaños que utilizan para infectar a los usuarios, de qué forma se propagan y cómo prevenirlas son algunos de los conocimientos que evitarán que un empleado sea infectado.
Una buena campaña de concientización no se logra con acciones esporádicas, por el contrario, es necesario una educación periódica y constante. La clave es no centrarse en un solo recurso, sino aprovechar cualquier oportunidad para educar. No solo se logra la concientización mediante charlas y cursos explicando los riesgos y las medidas de seguridad, además, se puede complementar con recordatorios periódicos de buenas prácticas, un boletín de noticias de actualidad, guías y manuales de configuraciones de privacidad y seguridad, o incluso videos y posters con consejos prácticos.

Medidas de concienciación para protegerse.

Es fundamental contar con una solución integral de seguridad que pueda detectar y bloquear amenazas conocidas de manera temprana. Actualizar aplicaciones y componentes del sistema operativo a su última versión, ya que el ransomware aprovecha vulnerabilidades. Los correos electrónicos son una importante fuente de propagación, por eso es importante evitar divulgar la dirección, revisar al remitente, cuidarse de ofertas tentadoras, verificar si se trata de un correo dirigido y filtrar los archivos ejecutables. Educar al personal para que no sucumba ante las técnicas de ingeniería social que se utilizan como puerta de entrada para la infección. Una adecuada política de backup asegurará la restitución de bases de datos y la continuidad del negocio incluso en las peores circunstancias.

Recomendaciones de Europol.

Partiendo de que el Ransomware una estafa diseñada para generar enormes ganancias para los grupos delictivos organizados, para prevenir y minimizar

los efectos del ransomware, el centro europeo de ciberdelincuencia de Europol aconseja tomar las siguientes medidas[54].

Actualizar el software regularmente. Muchos malware son el resultado de que los criminales explotan errores en el software (navegadores web, sistemas operativos, herramientas comunes, etc.). Mantenerlo actualizado puede ayudarlo a mantener seguros los dispositivos y archivos.

Usar software antivirus, instalar y mantener actualizado el software antivirus y de firewall en los dispositivos puede ayudar al ordenador a mantenerse libre de cualquier tipo de malware. Revisar siempre los archivos descargados con el antivirus.

Buscar y descargar software solo de webistes de confianza. Utilizar fuentes oficiales y sitios web recomendados para mantener el software parcheado con las últimas versiones de seguridad, y usar siempre la versión oficial de software.

Hacer una copia de seguridad regularmente de los datos almacenados en el ordenador. Copias de seguridad de datos completas ahorrarán mucho tiempo y dinero al restaurar el ordenador, incluso cuando se ve afectado por un ataque de ransomware.

Reportarlo, es decir, comunicar cuando se es víctima de ransomware, inmediatamente a la policía y al procesador de pagos involucrado. Cuanta más información se le dé a las autoridades, más eficazmente se podrá interrumpir la infraestructura criminal.

Consultar al proveedor de antivirus sobre cómo desbloquear y eliminar la infección del dispositivo. Existen numerosos sitios web y blogs oficiales con instrucciones sobre cómo eliminar de forma segura este tipo de malware de los dispositivos electrónicos. Es muy recomendable consultar www.nomereransom.org para verificar si ha sido infectado con una de las variantes de ransonware para las cuales hay herramientas de descifrado disponibles sin cargo.

[54] (Guía Europol. Ransomware, what you need to know. , 2016)

Lo que se debe evitar hacer.

Se debe evitar hacer clic en archivos adjuntos, banners y enlaces sin saber su verdadero origen, ya que lo que parece una publicidad o imagen inofensiva puede redirigir al sitio web desde el que se descarga el software malicioso. Lo mismo puede suceder al abrir archivos adjuntos en correos electrónicos recibidos de fuentes desconocidas.

Instalar aplicaciones móviles de proveedores o fuentes desconocidas. Hay que descargar siempre desde recursos oficiales y de confianza. En la configuración de los dispositivos Android, mantener siempre desactivada la opción "Fuentes desconocidas" y la opción "Verificar aplicaciones" marcada.

Dar algo por hecho. Si un sitio web advierte sobre software obsoleto, controladores o códecs (programas que codifican y decodifican los datos) instalados en el ordenador, no confiar plenamente en ellos. Para los delincuentes es muy fácil falsificar logotipos de empresas y software. Una búsqueda rápida en la web puede indicar si el software está realmente desactualizado.

Instalar o ejecutar software no confiable o desconocido. No instalar programas o aplicaciones en el ordenador si no se sabe de dónde vienen, ya que algunos tipos de malware instalan programas en segundo plano que intentan robar datos personales.

No pagar el dinero del rescate, ya que pagar no garantiza que el problema se resuelva y que se podrá volver a acceder a los archivos. Además, se apoya de esta manera el negocio de los ciberdelincuentes y el financiamiento de sus actividades ilegales.[55]

La complejidad de la solución ante un ataque de Ransomware.

[55] (Guía Europol. Ransomware, what you need to know. , 2016)

El ransomware está en auge, hay más de 50 familias de este malware en circulación actualmente y está evolucionando rápidamente. Con cada nueva variante se mejora el cifrado y se incorporan nuevas características.

Una de las razones por las que es difícil encontrar una solución es debido a que el cifrado en sí no es dañino. Realmente es una buena herramienta y muchos programas legítimos la utilizan.

El primer malware criptográfico utilizaba un algoritmo de clave simétrica, con la misma clave para cifrar y descifrar. La información corrupta podía ser descifrada con éxito normalmente mediante la ayuda de compañías de seguridad. Con el tiempo, los cibercriminales empezaron a utilizar algoritmos de cifrado asimétricos que utilizan dos claves diferentes, una pública para cifrar los archivos, y una privada necesaria para el descifrado.

El troyano *CryptoLocker* es uno de los ransomware más famosos, que utiliza también un algoritmo de clave pública. Cuando un ordenador es infectado se conecta con un panel de control para descargar la clave pública. La clave privada sólo la tienen los criminales que escribieron el software CryptoLocker. Normalmente, la víctima no tiene más de 72 horas para pagar el rescate antes de que la clave privada se borre para siempre, y resulta imposible descifrar ningún fichero sin esta clave.

Así que lo primero que hay que tener en cuenta es la prevención. La mayoría de los antivirus incluyen algún componente que ayuda a identificar el ataque de un ransomware en etapas tempranas de la infección, impidiendo la pérdida de información sensible. Es importante para los usuarios asegurar que esta funcionalidad está activada en el antivirus.

Es posible en determinados casos descifrar los archivos que fueron cifrados por el Ransomware cuando los autores del malware realizaron errores de implementación, haciendo posible romper el cifrado. Éste fue el caso del ransomware *Petya* y *CryptXXX*.
Cuando los autores del malware se sienten culpables por sus acciones y publican las claves, o una clave maestra, como en el caso de TeslaCrypt.

O cuando la policía captura servidores con claves y las comparten. Un ejemplo es *CoinVault*.

A veces pagar el rescate también funciona, pero no existe garantía de que realizar el pago permita descifrar tus archivos. Además, con esta acción se apoya el modelo de negocio de los criminales y en consecuencia se está coopera para que más gente se esté infectando con ransomware.

El número de usuarios que se han visto atacados por ransomware es inmenso, con unos 718.000 usuarios afectados entre abril de 2015 y marzo de 2016, esto significa que ha multiplicado su impacto x 5,5 veces comparado con el mismo periodo de tiempo en 2014-2015.

La policía no puede combatir el cibercrimen, y el ransomware en particular, por sí misma. Y los investigadores de seguridad no pueden hacerlo sin el soporte de las fuerzas del orden. La responsabilidad de combatir el ransomware está compartida entre la policía, los Gobiernos, Europol y las compañías de seguridad IT, y requiere un esfuerzo conjunto.

Herramientas de protección.

Si bien el ransomware pareciera ser la amenaza “de moda” en los últimos tiempos, son muchos los tipos de amenazas que se están propagando y afectando a los usuarios. Ya sea que se trate de un troyano, un gusano, un bot o el mismo ransomware, una buena herramienta integral de seguridad es capaz de prevenir la infección.

El término “antivirus” quedó acuñado en el subconsciente colectivo, este tipo de herramientas han evolucionado y pasaron de detectar solamente virus informáticos hasta convertirse en soluciones de seguridad completas, que proveen muchas otras funcionalidades como firewall, filtros de email y antispam, antiphishing o escaneo de memoria, entre otras, que dan una protección integral al sistema y permiten navegar seguro en el contexto actual de amenazas.

Por último, es importante actualizar regularmente los sistemas y aplicaciones, ya que muchas amenazas aprovechan vulnerabilidades no corregidas para propagarse por la red. Si bien esta tarea puede llegar a ser aburrida y rutinaria, existen herramientas de gestión de parches y actualizaciones que simplifican notablemente el trabajo.

Es importante destacar que ante una infección, la posibilidad de recuperar la información y la forma de hacerlo dependerá del tipo de amenaza específica.

En general, en los casos del tipo lockscreen es posible recuperar el acceso al sistema limpiando la infección o restaurando el equipo. Además, en estos casos, si los archivos no son cifrados es posible recuperarlos del disco afectado.
Sin embargo, en algunas variantes especialmente aquellas que afectan dispositivos móviles, el bloqueo no permite la recuperación del equipo, por lo que la única solución terminará siendo un reseteo de fábrica, borrando toda la información. En el caso de los filecoders la recuperación puede ser más complicada.

En la mayoría de los casos, un buen software de seguridad tendría que ser capaz de quitar el ransomware del equipo, los archivos seguirán cifrados. En algunas familias de ransomware, especialmente las que utilizan el cifrado simétrico y guardan la clave dentro del código malicioso, es posible recuperar los archivos utilizando la herramienta específica de descifrado. Sin embargo, los archivos que fueron atacados por un tipo más sofisticado de ransomware, como Cryptolocker, son imposibles de descifrar sin la clave correcta. En cualquier caso, si ocurre una infección es recomendable limpiar el equipo de la infección, ya sea utilizando una herramienta de seguridad o reinstalando el sistema, y luego recuperar la información y los archivos mediante un respaldo limpio.

[56] (Guía Europol. Ransomware, what you need to know. , 2016)

Pagar el rescate no es garantía de recuperar los archivos.

La realidad es que recuperar los archivos no está garantizado. Si se cuenta con la clave maestra se van a poder descifrar todos los documentos, no obstante, conseguir la clave sin ceder ante el pago de los cibercriminales es lo complejo. Si bien existen variantes de cryptolockers para las cuales es posible descifrar y recuperar los archivos afectados, en la mayoría de las ocasiones esto resulta casi imposible, sobre todo si el algoritmo es fuerte; la clave no puede ser obtenida a partir del código del malware; y las claves maestras son únicas para cada víctima y funciona solo para un equipo[57].

3. Formación y reciclaje de los perfiles de riesgo.

En cuanto a los fabricantes, es importante hablar sobre el "Zero Day", que se trata de las vulnerabilidades de los programas desconocidas para su fabricante, por tanto, no han podido emitir un parche que la subsane. Esto supone estar desprotegidos contra ellas ya que son desconocidas para los equipos que administran los sistemas. Ante estas vulnerabilidades las protecciones más efectivas son el aislamiento, es decir, cortar internet, o bien la concienciación, es decir, sospechar de un correo extraño o no solicitado. De esta forma evitamos, por ejemplo, que un archivo se copie entre todos los ordenadores vulnerables de una red. Este es el caso de WannaCry.

La RansomSociety.

Es la sociedad secuestrada por la amenaza de este tipo de acciones, cada día hay más preocupación por la "amenaza digital", se han visto robos de información que han influido en resultados electorales, países que abandonan las máquinas para hacer el recuento de sus elecciones "analógicamente"

[57] (Guía Europol. Ransomware, what you need to know. , 2016)

(Holanda) por miedo a intervenciones de un tercero. Ataques a infraestructuras críticas con éxito.
La amenaza existe, y más desde que ha pasado a tener plan de negocio. Conviene recordar que la “industria” del malware mueve miles de millones de euros actualmente, por tanto, hay negocio y hay gente dispuesta a beneficiarse de este mercado.

Amenazas futuras y su desarrollo.

Incluso antes del brote de WannaCry, el ransomware ya estaba establecido para tomar el escenario central en términos de amenazas de malware.
La escala y la amplia superficie del ataque WannaCry fue sin precedentes, ya que muy pocos fueron los países que no se vieron afectados.
El aspecto positivo de esto es la generación de un despertar global, concienciar sobre la amenaza en todo el mundo y crear una oportunidad para que los problemas de seguridad de las TI (Tecnologías de la información) sean tomados más en serio por empresas y organizaciones, incluida la necesidad de mejorar la gestión de parches y vulnerabilidades.

La seguridad cibernética es una industria en crecimiento, y dentro de Europa es probable que las primas de seguros aumenten a 8.900 millones de euros en 2020 desde alrededor de 3.000 millones de euros en la actualidad.

Hay un evidente riesgo de seguridad cibernética fomentando la necesidad de suscribir seguros para tener así alguna garantía, ya que los riesgos son inevitables, sobre todo en el caso de aquellas empresas y organizaciones que dependen de estos seguros para cubrir pérdidas potenciales en lugar de invertir en acciones preventivas medidas.

Un elemento clave ocurrido tanto en el ataque de WannaCry y el ataque de Petya/NotPetya fue la inclusión de la auto-propagación o la funcionalidad 'gusano' dentro del malware, creando lo algunos se refieren a como un 'ransomworm'. Si bien esto no fue la primera vez que esto se ha hecho, es el

ejemplo más exitoso de su implementación, y una táctica que probablemente se repetirá en futuras amenazas.

Los troyanos bancarios no figuraban en gran medida en los informes policiales del año 2016, sin embargo, su desarrollo e innovación no cesa de aumentar. Como se informó en años anteriores, hay poco en el camino del malware completamente nuevo, ya que los desarrolladores se centran en las variantes ya existentes, como la variante Zeus Panda, o la variante Dyre Trickbot, o malware híbrido que combina aspectos de otras variantes exitosas, como Goznym que toma prestado tanto del troyano bancario Gozi como del Nymaim descargador.

Los ataques sofisticados contra las infraestructuras críticas europeas son una amenaza real. Sin embargo, los ataques, tanto directos como indirectos, contra infraestructuras críticas utilizando el ataque cibernético comúnmente disponible herramientas como booters/stressers parecen ser mucho más probable y más fáciles de detectar.

Si bien estos ataques pueden no ser tan dañino como derribar una red eléctrica, pueden causar la interrupción severa y el colapso de servicios clave. La directiva de seguridad de la información de red (NIS) establece las soluciones de ciberseguridad en los sectores críticos, requiriendo identificar a los operadores de estos sectores para tomar las medidas apropiadas y proporcionadas para gestionar los riesgos que plantea la seguridad de sus redes y sistemas de información, incluida la necesidad de notificar incidentes significativos. Como tal, se espera que la directiva NIS tenga un impacto fuerte y positivo en la ciberseguridad de las infraestructuras críticas.

Conclusiones y opinión personal.

Se debe llevar a cabo una regulación y tipificación exhaustiva de los diferentes delitos informáticos que han surgido debido a la evolución de la informática y del crimen a través de estos medios.

La concienciación de los usuarios, de los ciudadanos que hacen uso de internet en sus hogares, y de las empresas y organizaciones, tanto públicas como privadas, es necesaria para prevenir y saber actuar en caso de ser víctimas de cualquier ataque o ciberdelito.

Se deben adoptar medidas que frenen a los posibles autores de dichos delitos, así como sanciones a tales conductas.

Poner a disposición todo tipo de herramientas y formación necesaria para difundir así técnicas de prevención y protección. Además de hacer hincapié en denunciar en el plazo más breve posible en caso de ser víctimas de cualquier ciberataque.

Concienciar de que el pago del rescate solo consigue incentivar más a los ciberdelincuentes, ya que saben que es un método cómodo, seguro y eficaz de conseguir dinero, información, dañar la imagen y reputación de empresas y particulares, etc.

Y, por último, dar a conocer y difundir en qué consisten las técnicas de ingeniería social, ya que el factor humano es el eslabón más débil en la seguridad de la información.

Personalmente, opino que el continuo auge de los ciberdelitos y los graves perjuicios que causa a la población son un asunto de suficiente entidad como para que estén en el foco de la actualidad con más intensidad y protagonismo del que goza hoy en día, que es prácticamente nulo.

Tras realizar el trabajo, considero que estamos ante una alarma social que está pasando desapercibida porque gran parte de la población todavía no es

consciente de los riesgos a los que está expuesta mientras hace uso de sus dispositivos.

La cifra de víctimas y de ataques que se llevan a cabo a diario, junto al volumen de capital económico ilícito que obtienen y manejan los ciberdelincuentes, puede derivar en graves problemas sobre todo para los usuarios domésticos, ya que los profesionales de la informática, los usuarios con conocimientos avanzados y las empresas y corporaciones conocen el riesgo real y grave al que están expuestos.
Empresas como Facebook pagan cantidades millonarias a quienes detecten cualquier agujero de seguridad en sus servicios y aplicaciones, ya que son conocedores de que cualquier filtración de datos podría hacerles desaparecer como red social (Facebook tiene $300.000 *millones* de valoración bursátil).

Internet y las nuevas tecnologías forman parte de nuestra vida diaria desde edades cada vez más tempranas, por tanto, considero que sería una buena técnica de prevención el introducir en el sistema educativo una asignatura que tratara las nuevas tecnologías y los riesgos a los cuáles nos exponemos con su uso, destacando sus beneficios y sobre todo sus aspectos negativos, para así ser conscientes de que todos los usuarios de internet somos víctimas potenciales de cualquier malware.

Considero que, realizando un esfuerzo conjunto entre el Gobierno, las fuerzas y cuerpos de seguridad y los profesionales de la seguridad informática se pueden prevenir y disminuir en gran medida las infecciones a los sistemas y dispositivos que en muchas ocasiones los propios usuarios instalamos de manera inconsciente.

Además de víctimas nos convertimos en una especie de cómplices de los ciberdelincuentes por pagar el rescate que nos solicitan ya que solo favorecemos la continuidad de sus ataques.

Por último, creo que se debe motivar a la población a que denuncie, ya que la mayoría de las infecciones no se ponen en conocimiento de la policía ni de las autoridades judiciales. Las víctimas prefieren sufrir las consecuencias del delito

e intentar prevenirlo para el futuro, antes que iniciar un procedimiento judicial, y esto dificulta el conocimiento preciso del número de delitos cometidos y con ello la planificación de las adecuadas medidas legales sancionadoras o preventivas.

BIBLIOGRAFÍA

GARCÍA LÓPEZ, A. Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio. Publicado el 20 junio de 2016. Disponible en: http://www.alfredogarcialopez.es/penal-4/

MAEZTU, D. “Tipificación penal del ransomware”. Publicado el 12 de mayo de 2017. Disponible en: http://www.derechoynormas.com/2017/05/tipificacion-penal-del-ramsomware.html

PLATAFORMA DE AFECTADOS POR EL VIRUS DE LA POLICÍA. [Consulta: mayo 2018]. Disponible en: https://asociacionafectadosinternet.es/plataforma-de-afectados/plataforma-virus-de-la-policia/

NIST Cybersecurity Framework vs ISO 27001. A través de ¿Cybersecurity Framework o ISO 27001? Publicado el 24 de febrero de 2018. Disponible en: http://noticiasseguridad.com/seguridad-informatica/cybersecurity-framework-o-iso-27001/ y https://blog.segu-info.com.ar/2018/03/nist-cybersecurity-framework-vs-iso.html

MENDOZA, M.A. La evolución del ransomware: del ochentero PC Cyborg a un servicio en venta. Publicado el 21 de agosto 2015. Disponible en: https://www.welivesecurity.com/la-es/2015/08/21/evolucion-del-ransomware/

ESET Latinoamérica. 28 de Julio de 2015. ¿Qué es el ransomware y cómo afecta a los entornos corporativos? [Consulta: Mayo 2018]. Disponible en: https://www.welivesecurity.com/la-es/infographics/que-es-el-ransomware-y-como-afecta-a-los-entornos-corporativos/

DEFINICIONES GLOSARIO. Disponible en: https://www.welivesecurity.com/la-es/glosario/

NO MORE RANSOM. 2018. [Consulta: Mayo 2018] Disponible en: https://www.nomoreransom.org/es/ransomware-qa.html

INFORME DE LA UNIÓN EUROPEA SOBRE CIBERDELINCUENCIA. 26 DE JULIO DE 2017. Disponible en: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0272+0+DOC+XML+V0//ES

CUESTA MARTINEZ, F. COBIT 5: Marco de negocio para seguridad de la información. Publicado el 30 de septiembre de 2015. Disponible en: https://riunet.upv.es/handle/10251/56417?show=full

REGLAMENTO UE 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 27 DE ABRIL DE 2016, RELATIVO A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESOS DATOS Y POR EL QUE SE DEROGA LA DIRECTIVA 95/46/CE. Disponible en: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

ACOSTA DAVID, E. Guía rápida para entender el marco de trabajo de ciberseguridad del NIST.- CISSP Instructor, CISM, CISA, CRISC, CHFI Instructor, CEH, PCI QSA, OPST, BS25999 L. A. Publicado el viernes, 23 de diciembre de 2016. Departamento de Consultoría Disponible en: http://blog.isecauditors.com/2016/12/guia-rapida-para-entender-marco-trabajo-de-ciberseguridad-del-NIST.html

KARCZEWSKA, J. CISA. COBIT 5 y el reglamento RGPD. COBIT Focus. Publicado el 29 de marzo de 2017. Disponible en: http://blog.isecauditors.com/search?q=ransomware y http://www.isaca.org/COBIT/focus/Pages/cobit-5-and-the-gdpr-spanish.aspx

NEIRA LÓPEZ, A. Lead Tutor y Técnico especialista en formación desarrolla e imparte programas en Diseño y Mejores Prácticas en la gestión de los Data Center. Auditor jefe de certificación para ISO 27001, ISO 20000, ISO 22301

(BS25999) con acreditaciones ENAC, UKAS e itSMF, así como, esquemas de evaluación de disponibilidad (TIER) y eficiencia energética (CEEDA) para Data Center.
SPOHR RUIZ, J. Ingeniero de Telecomunicación, CISA, Lead Auditor ISO 27001 y ISO 22301 (BS25999). Lead Tutor ISO 27001. Auditor jefe de certificación de ISO 27001. Auditor Jefe de Calidad de Servicio y Calidad de Facturación en operadores de telecomunicaciones, según Orden Ministerial ITC/912/2006.
Disponible en: www.iso27000.es

MILTON, S. CISA, CGEIT. “COBIS FOCUS”. Publicado el 3 de abril de “017. Cómo COBIT 5 puede ayudar a reducir la probabilidad y el impacto de las 5 amenazas cibernéticas más importantes. Disponible en: http://www.isaca.org/COBIT/focus/Pages/how-cobit-5-can-help-reduce-the-likelihood-and-impact-of-the-top-5-cyberthreats-spanish.aspx

GUÍA IOCTA 2017. Disponible en: https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwi-2NrPxq3cAhWS-aQKHdAiApwQFggoMAA&url=https%3A%2F%2Fwww.ccn-cert.cni.es%2F%3Fid%3D4795%3Aguia-sobre-la-seguridad-en-redes-inalambricas%26start%3D44&usg=AOvVaw1xek8bd6n-D_bEKW2HWXtI

GUÍA REGLAMENTO DE PROTECCIÓN DE DATOS 2018. Disponible en: https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiss-Lmxq3cAhVN3qQKHcT0C34QFggpMAA&url=https%3A%2F%2Fwww.aepd.es%2Fmedia%2Fguias%2Fguia-rgpd-para-responsables-de-tratamiento.pdf&usg=AOvVaw3RkIeEY6tPqxPw5aA_79j_

INCIBE. Productos antimalware. Publicado el 05/06/2018. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/protegiendo-nuestra-empresa-productos-anti-malware?utm_campaign=empresas&utm_medium=twitter&utm_source=post

GÓMEZ REY, H. Abogado del Área Governance, Risk and Compliance de Ecix. “Brechas de seguridad y ransomware wannacry”. Disponible en: https://www.ecixgroup.com/brechas-seguridad-nuevo-reglamento-general-proteccion-datos-proposito-del-ransomware-wannacry/

ÉCIJA, Á. Ecix Group. Publicado en Madrid el 12 de mayo de 2017. “Ransomware delito de estafa en concurso con delito informático”. Disponible en: https://cincodias.elpais.com/cincodias/2017/05/12/legal/1494614621_922741.html

CUERVO ÁLVAREZ, J. Delitos informáticos: Protección Penal de la Intimidad. 1 de enero de 2014. Disponible en: http://www.informatica-juridica.com/trabajos/delitos-informaticos-proteccion-penal-de-la-intimidad/#5.%20CONDICIONES%20OBJETIVAS%20DE%20PERSEGUIBILIDAD.%20ART.

MUÑOZ DEIROS, E. Delito contra la protección de datos. Disponible en: https://evamunoz.es/delito-contra-la-proteccion-de-datos-habeas-data/

OBSERVATORIO ESPAÑOL DE DELITOS INFORMÁTICOS. 2018. [Consulta: Mayo 2018].

Disponible en: http://oedi.es/

INFORME CRIMINALIDAD 2015 DEL MINISTERIO DEL NITERIOR. Disponible en: https://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjl-faCx63cAhWS6qQKHaW5C4cQFggpMAA&url=http%3A%2F%2Fwww.interior.gob.es%2Fdocuments%2F642317%2F1204854%2FAnuario-Estadistico-2015.pdf%2F03be89e1-dd38-47a2-9ce8-ccdd74659741&usg=AOvVaw2L6JS4Mg6kNi0QUo2n3JUO

SAN JOSÉ, J. “SIRIUS, la plataforma de Europol para facilitar las investigaciones de los ciberdelitos”. Disponible en: https://derechodelared.com/2017/11/02/sirius/

RTVE.es / EFE. 01.02.2018. *“Los españoles pasan más de cinco horas diarias conectados a internet”.* [Consulta: junio 2018]. Disponible en: http://www.rtve.es/noticias/20180201/espanoles-pasan-mas-cinco-horas-diarias-conectados-internet/1671382.shtml

ANEXO. Glosario de términos.

TOR: Tor es un software libre y una red abierta que lo ayuda a defenderse contra el análisis del tráfico, una forma de vigilancia de la red que amenaza la libertad y la privacidad personal, las actividades y relaciones comerciales confidenciales y la seguridad del estado.

BITCOIN: Se trata de una moneda virtual (criptomoneda). Se emplea tanto en transacciones financieras realizadas a través de ellas en el mundo virtual, así como medio de pago en caso de ataques.

Cibercrimen: Actividad delictiva organizada que implica el uso de herramientas informáticas y se basa en Internet para su ejecución. El objetivo es obtener beneficios, por lo general financieros. Delitos tales como el phishing, scam o robo de identidad son considerados cibercrimen, como así también todos los recursos y actores que forman parte de su circuito criminal.

Ciberdelincuente: Persona que comete cibercrimen.

Deep Web: Conjunto de sitios web y bases de datos que forman parte de Internet, pero que escapan (de manera deliberada o no) a la indexación de los motores de búsqueda, y que por tanto se consideran de difícil acceso.

Ingeniería Social: Conjunto de técnicas utilizadas para engañar a un usuario a través de una acción o conducta social. Consiste en la manipulación psicológica y persuasión para que voluntariamente la víctima brinde información personal o realice algún acto que ponga a su propio sistema en riesgo. Suele utilizarse este método para obtener contraseñas, números de tarjetas de crédito o PIN, entre otros.

Phishing: uno de los métodos ms utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta´, como puede ser una contraseña o información detallada sobre tarjetas de crédito, u otra información bancaria de la víctima.

Malwertising: se trata de anuncios donde **los atacantes ocultan en la publicidad el código malicioso** y no es necesario hacer click o descargarlo para infectarse.

Cryptoware: Es la encriptación del ransomware, se ha convertido en la amenaza de malware más intensa, eclipsando el robo de datos malware y troyanos bancarios. Con el criptoware convirtiéndose una amenaza clave para los ciudadanos y las empresas, la aplicación de la ley y la industria de seguridad de internet ha respondido rápidamente y en concierto, con prevención y conciencia campañas y asistencia técnica, y operaciones dirigidas los grupos criminales y la infraestructura involucrada.