MALWARE: UNA PUERTA A LA CIBERCRIMINALIDAD

José Antonio Córdoba Bahamón
joancoba@hotmail.com
Universidad Piloto de Colombia

Resumen—El documento aborda una de las nuevas formas de criminalidad, la cual, a través de dispositivos, computadores, incluso, cualquier tipo de sistema que se encuentre conectado al internet, ha permitido que delincuentes roben, e incluso, secuestren información a grandes organizaciones o personas del común. También expone el aumento de estos casos que se ubican no solo en Colombia, si no también en el mundo y cómo contrarrestar o prevenir dicha problemática.

Abstract— The paper addresses one of the new forms of criminality, which across devices, computers, even, any system that is connected to the Internet, has allowed criminals to steal, and even hijack information to large organizations or people common. It also exposes the increase of these cases are located not only in Colombia, but also in the world and how to counteract or prevent such problems.

Índice de Términos—Malware, cibercriminales, ciberespacio, bitcoin, información, tecnología, internet, cifrado de información, Deep web, leyes.

I. INTRODUCCIÓN

Expertos en el tema encontraron una forma de cometer actos ilícitos de forma virtual. Es así como más personas, de manera individual o por medio de agrupaciones criminales, utilizan y aprovechan el desconocimiento o posibles puertas abiertas que les brinda la red, para apropiarse de información, la cual es utilizada para obtener un sinnúmero de beneficios mediante el secuestro y la extorsión.

La criminalidad en la actualidad no solo nos asecha en las calles, desde la invención de la Internet, sus usuarios, que no solo pertenecen a las nuevas generaciones denominadas los millennials, personas nacidas desde los 80, sino también aquellas que se han visto en la obligación de enfrentarse a estas, se encuentran expuestos cada vez que ingresan una clave, envían un correo o descargan un archivo.

Esta nueva tendencia, nos lleva a pensar en diseñar e instaurar nuevas leyes, normas y protocolos de uso, para la navegabilidad segura, en una plataforma que contempla espacios impensables.

Hace algunos años el temor más grande es que ladrones lograran secuestrar nuestros seres queridos, ahora este temor se traslada a un escenario virtual, en donde la información está a la merced de personas inescrupulosas.

Con este documento pretendo abordar los diferentes conceptos que nos harán entender cómo funciona la ciber-criminalidad y, lo más importante, qué debemos hacer ante esta creciente propagación de delincuentes, que de manera permanente encuentran formas de acceder a nuestros archivos personales.

Y es que entre más nos rodemos de cosas que tengan la posibilidad de conectarse a la red, menor es la posibilidad de blindarnos ante actos delictivos.

Así mismo, hablamos sobre la importancia de la información y el papel que juega en este momento en el panorama empresarial, social y gubernamental.

Una mirada precisamente a la regulación actual para la protección de la misma, ya que esta puede contenerse en cualquier tipo de dispositivo y ser utilizada para otros fines de manera arbitraria.

Este tema es sin duda alguna una construcción continua del estudio de comportamientos en el uso de las tecnologías, ya que de manera constante se reinventa, lo que expone a sus usuarios.

II. LA AMENAZA DETRÁS DE UNA TECNOLOGÍA QUE ATENTA EN CONTRA DE LAS PERSONAS

A partir de los destrozos que han dejado a su paso las diferentes guerras, las cuales tuvieron lugar en el viejo mundo, hoy gozamos de diversas tecnologías, las cuales nos facilitan en una gran medida la manera de hacer las cosas. Y es que las guerras han sido los puntos de partida para el desarrollo de inventos que nos faciliten la vida, desde diferentes campos: medicina, cibernética, robotización, ingeniería genética y biotecnología, informatización y telecomunicaciones.

Con respecto a este tema, Rodrigo D. Rodríguez Angulo asegura que *"la historia de las guerras (más de 14 000 guerras en 30 siglos) muestra que su alcance e impacto social ha ido creciendo y que siempre ha tenido una estrecha relación con el desarrollo de la ciencia y la tecnología".*

Para este caso nos atañe en gran medida uno de los inventos que revolucionó la vida misma y la forma en que las personas interactúan con las "nuevas cosas": la internet, la cual juega un papel muy importante, ya que además de acorta las distancias en materia de comunicación, es el mayor archivador de información, tanto personal como empresarial y gubernamental.

Pero qué es, pues bien, se puede decir que la internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan los protocolos TCP/IP o como lo define Manuel Castells, *"Internet es el tejido de nuestras vidas en este momento. No es futuro. Es presente. Internet es un medio para todo, que interactúa con el conjunto de la sociedad".*

Sus orígenes se remontan a 1969, y se les atribuyen a tres universidades de California (Estados Unidos), las cuales lograron una conexión en simultánea, y a los programas de investigación militar [1].

Este tipo de conexión, que cada vez es más veloz, interconecta numerosos dispositivos, tales como: celulares, tablets, computadores, vehículos, entre otros, a través de los cuales se depositan archivos que van desde fotografías personales, hasta datos, claves, números privados, direcciones, números de cuentas, grabaciones, mensajes de voz, mensajes SMS, correos electrónicos, etc.

Lo anterior, les permite a terceros acceder a esos datos, que exponen a la empresa y, por su puesto, a las personas del común.

En la actualidad, existen denuncias de todo tipo que pone entre ojos la seguridad de conectarnos a la red. Según un artículo publicado en marzo de este año por El Espectador:

"En 2015, por ejemplo, se registraron 7.118 ciberataques y, según el Departamento de Delitos Informáticos de la Policía, entre 2014 y el año pasado hubo un aumento del 40%. Las pérdidas económicas derivadas por estos actos representan(ron) al país alrededor del 0,14% del PIB Nacional (en 2014), es decir, cerca de US$ 500 millones aproximadamente, explicó Telefónica, basándose en datos que recogió el Banco Mundial. En pesos colombianos, la cifra sería de más de $1.500 millones, cifra confirmada por el Ministerio de Tecnologías de la Información y las Comunicaciones" [2].

De igual manera, Digiware, una empresa de seguridad informática, presentó un estudio sobre incidentes cibernéticos en Latinoamérica.

Entre los hallazgos, "*Colombia representa el 21,73 por ciento dentro de los países que más reciben ataques cibernéticos en América Latina; seguido por Argentina con un total de 13, 94 por ciento y Ecuador junto a Perú con un 11, 22 por ciento"* [3].

Frente a esta creciente problemática en el mundo, la Unión Europea UE y la Organización del Tratado del Atlántico Norte OTAN han firmado un acuerdo para reforzar la cooperación contra ataques cibernéticos, los cuales aumentaron en 2015 un 20 por ciento en Europa y Norteamérica.

A través de la red no solo roban dinero de las cuentas bancarias, recientemente, existe una modalidad en donde la información es secuestrada, gracias a un programa informático malicioso que, una vez se instala en el ordenador, provoca que los archivos o partes del sistema afectados no se abran o que el acceso a los mismos esté restringido, pidiendo un "rescate" para que el usuario pueda volver a tener el control sobre ellos [4].

El 'malware', como se le denomina se ha convertido en una amenaza electrónica que "aterroriza" a sus posibles víctimas, sus fotos, sus datos, sus correos son suficientes para que un posible estafador logre estudiar a su víctima, para así llevar a cabo de manera exitosa una extorsión efectiva.

Frente a este panorama, la pregunta sería: ¿Las organizaciones y las personas están preparadas para enfrentar el cibercrimen?

III. EL OSCURO MUNDO QUE ESCONDE LA DEEP WEB

Así como en el mundo, existen graves problemáticas que se esconden detrás de la legalidad, la internet aguarda un mundo paralelo y oscuro, el cual oculta delitos que van desde la pornografía infantil, hasta contratación de asesinos a sueldo.

Pero qué es Deep Web, como comúnmente se conoce, pues bien, el BrightPlanet, un grupo que se especializa en inteligencia lo define como: *"cualquier cosa que un motor de búsqueda no pueda encontrar",* según un estudio en el Journal of Electronic Publishing, *"el contenido de la Deep Web es masivo, aproximadamente 500 veces más grande de lo que es visible y que se encuentra en los motores de búsqueda tradicionales"* [5].

Entre los actos ilícitos que se pueden encontrar están:

- ***Servicios financieros:*** *lavado de bitcoins, cuentas de PayPal robadas, tarjetas de crédito clonadas, falsificación de billetes, carteras de dinero anónimas.*
- ***Servicios comerciales:*** *explotación sexual y mercado negro: gadgets robados, armas y munición, documentación falsa y —sobre todo— drogas.*
- ***Servicios de hosting:*** *alojamiento web y almacenamiento de imágenes donde se antepone la privacidad.*
- ***Blogs, foros y tablones de imágenes:*** *aparte de las vinculadas a los servicios de compraventa, dos categorías frecuentes de este tipo de comunidades son el hacking y el intercambio de imágenes de toda clase.*
- ***Servicios de correo y mensajería:*** *algunas direcciones de email son gratuitas (generalmente sólo ofrecen webmail) y otras de pago, con SSL y soporte de IMAP. La mayoría de servicios de chat funcionan sobre IRC o XMPP.*
- ***Activismo político:*** *intercambio de archivos censurados, hacktivismo y hasta una página para organizar "magnicidios financiados en masa".*
- ***Secretos de Estado y soplones:*** *hay un mirror de WikiLeaks en la Deep web, y varias páginas donde publicar secretos con poca actividad. Lo más interesante es una web sobre los túneles secretos de la universidad de Virginia Tech.*
- ***Páginas eróticas:*** *de pago y de libre acceso. Las subcategorías son variopintas y sin ningún límite moral [6].*

Por otra parte, es pertinente hablar sobre las ventajas de la deep web, la cual les ofrece a las personas un mundo en un anonimato real, en donde les permite expresarse sin riesgos, navegar libremente sin que se guarden los datos de lo que ven y visitan, acceder a investigaciones científicas y hasta libros censurados por el gobierno.

También puede ser una herramienta muy útil para el gobierno en el monitoreo de crímenes por bandas delincuenciales, terrorismo y actividades ilícitas.

La gran desventaja de esta web es que usuarios del común son algo ingenuos y algunos por desconocimiento propio, no saben que la gran mayoría de usuarios conectados son principalmente hackers. Como bien se sabe estos expertos en informática usan sus habilidades para el robo de datos en la Deep Web.

Entre los delitos enumerados anteriormente, existen hackers a sueldo, que realizan cualquier tipo de trabajo, estos de dividen en las siguientes tres categorías:

A. Sombreros Blancos (White Hats): *También conocidos como hackers éticos utilizan sus conocimientos para defenderse y por lo general son aquellas personas profesionales de la seguridad informática, aplicando sus conocimientos encuentran distintos tipos de vulnerabilidades y realizan las acciones correspondientes para corregir a las mismas.*
B. Sombreros Negros (Black Hats): *También conocidos como cibercriminales, tiene vastos conocimientos de la informática, que los utilizan para el desarrollo de herramientas de búsqueda de vulnerabilidades, desarrollan código para obtener un beneficio de ello.*
C. Sombreros Gris (Grey Hats): *Son aquellas personas, que tienen conocimientos y los utilizan según les convenga o quieran. Por lo general para sus propósitos utilizan herramientas desarrolladas por los black hats.*

IV. EL DINERO VIRTUAL QUE COMPRA AL MUNDO “BICOINT”

Bitcoin es una moneda digital descentralizada, creada en el 2009 por Satoshi Nakamoto. Es descentralizada porque no depende de un organismo central que se encargue de emitirla.

Las transacciones se realizan de la siguiente manera:

a) El usuario receptor de los Bitcoin le envía su clave pública a quien desea transferir su Bitcoin.
b) El usuario que desea enviarle los Bitcoin agrega en la transacción la clave pública que le envió el destinatario con el monto que desea enviar.
c) Por último el usuario que realizar el pago debe firmar la transacción con su clave privada secreta, esto por garantizar que es ella. Minutos después que la transacción fue replicada, con todos los detalles de la transacción, a todas las máquinas que esté disponible en la red P2P, el usuario receptor verá reflejada la transacción en su saldo [7].

Para utilizar Bitcoin se requiere convertir el dinero en un monedero virtual para almacenarlo, que no es más que una dirección en la que se almacena Bitcoins, para acceder a ello, tan solo se debe ingresar a servicios gratuitos que existen, como por ejemplo Blockchain o WalletBit, y crear el monedero asociando un nombre de usuario y una contraseña.

Esta forma de pago permite que lo ilegal pueda quedar en lo oculto y así, las personas que acuden a servicios ofrecidos en la Deep Web puedan moverse de manera sigilosa.

V. UN INVENTO QUE LE ABRE ESPACIO AL CIBERCRIMEN

Para definir este concepto, es importante precisar que las palabras que la componen: CIBER y CRIMEN, son definidas por la Real Academia Española (RAE), como CIBER: 'cibernético'. Ciberespacio, cibernauta", y CRIMEN: "delito grave", "acción indebida o reprensible" o " acción voluntaria de matar o herir gravemente a alguien".

Lo anterior, nos define cibercrimen como un delito o acción indebida que realiza en el ámbito artificial a través de medios informáticos (Ciberespacio).

Según, Serrano Maíllo, en su libro Introducción a la criminología, le refiere el término cibercrimen al comportamiento concreto que reúne una serie de características criminológicas relacionadas con el ciberespacio.

Según, Hernández Díaz, los delitos más conocidos de un cibercriminal son:

a) Fraudes financieros.
b) Entrada no autorizada a sitios web.
c) Espionaje industrial.
d) Pornografía infantil.
e) Crímenes de mayores dimensiones como acoso sexual, secuestros, extorsiones y actividades relacionadas con el narcotráfico.

También podemos traer a colación el “Convenio sobre la Ciberdelincuencia”, el cual fue firmado el 1 de noviembre de 2001 en Budapest.

En este convenio se propone una clasificación de los delitos informáticos en cuatro grupos, pero mencionaremos dos de ellos, los cuales nos atañe en el presente documento:

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

- Acceso ilícito a sistemas informáticos.
- Interceptación ilícita de datos informáticos. Interferencia en el funcionamiento de un sistema informático.

- Abuso de dispositivos que faciliten la realización de delitos.

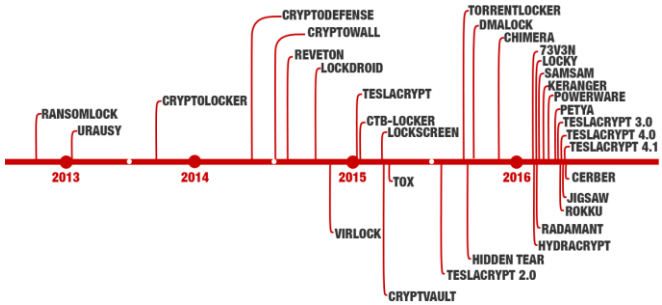

Figura 1: Línea de tiempo de aparición de Ransomware. [8].

- Falsificación informática mediante la introducción, borrado o supresión de datos informáticos.
- Fraude informático mediante la introducción, alteración o borrado de datos informáticos, o la interferencia en sistemas informáticos.

VI. MALWARE: EL VIRUS VIRTUAL QUE ESCONDE LA INTERNET

Los códigos o software malicioso, software malintencionado o malware, son programas que se crean para modificar la conducta habitual de un programa, para entorpecer o bloquear sus funciones, sin que el usuario víctima sea consciente de ello.

Existen tres tipos de malware: virus, gusanos y troyanos.

a. Virus: *infectan otros archivos, por lo que solo pueden existir en un equipo si se hallan dentro de otro fichero. Los ficheros infectados generalmente son ejecutables, pero también pueden infectar otros archivos que se hallen en el propio equipo infectado.*

Los virus pueden ejecutarse cuando el usuario ejecute un fichero que se halle infectado, o si están programados para ello, cuando se realice una determinada acción o se cumpla una determinada condición (por ejemplo, una fecha concreta, una cuenta atrás, etc.). El mecanismo de los virus básicamente es el infectar a otros ficheros con las mismas características que él mismo, así, las posibilidades de propagación son infinitas.

b. Gusanos: *son programas maliciosos que basan su funcionamiento en realizar el máximo número de copias de sí mismos, con el objetivo de crear una propagación masiva. La principal diferencia respecto a los virus es que no infectan otros ficheros que se alojen en el equipo víctima. Los principales métodos de propagación de este tipo de malware son los correos electrónicos, las redes P2P15, la mensajería instantánea y los canales de chat.*

Generalmente los creadores de este tipo de malware utilizan la ingeniería social16 para alentar al usuario receptor a usar el fichero infectado con el gusano. Así, los infractores generalmente intentan poner un título atractivo para la mayor cantidad de usuarios posibles a los archivos que contienen un gusano. Si se trata de las redes P2P, pueden nombrar al archivo con títulos de discos de música de actualidad, o si se trata de un correo electrónico, con ofertas sugerentes o temas que atraigan la atención del usuario medio.

c. Troyanos: *Software malicioso caracterizado con aspecto de programa legítimo, pero que al ejecutarse crea una puerta trasera que permite la administración remota del equipo a un usuario no autorizado. Carecen de rutina propia de propagación, pueden llegar al sistema de diferentes formas.*

En sus orígenes, la aparición de troyanos iba encauzada a realizar el máximo daño posible en el equipo infectado. Una vez que se había ejecutado el troyano, el infractor podía manejar el equipo infectado de forma remota, pudiendo realizar todo tipo de acciones tales como borrar información de los discos duros, ocupar los discos duros con archivos superfluos, realizar capturas de pantalla, monitorizar pulsaciones del teclado, instalación de otros programas en el equipo infectado, etc.

El funcionamiento de los troyanos se basa en tres programas: un cliente, que es el que dirige al equipo infectado y va ordenando cada uno de los movimientos a realizar, un servidor situado en la computadora infectada, que recibe y ejecuta las órdenes que le va suministrando el cliente, y en función de los resultados obtenidos, devuelve un resultado al programa cliente, y por último un editor del servidor, que tiene como principales funciones la modificación del servidor, la protección del mismo (por ejemplo, a través de contraseñas) y el desarrollo de otras actividades como la unión del servidor a otros programas para que al abrirlos se ejecute, configurar en el puerto donde se instalará, etc. [9].

VII. RANSOMWARE

Se traduce como ransom, 'rescate', y ware, por software, es un tipo de programa informático malintencionado, el cual restringe el acceso a determinadas partes o archivos del sistema infectado.

Es en este punto es donde las personas se pueden convertir en blancos fáciles, ya que, a través de este tipo de programa, le permite al delincuente pedir un rescate a cambio de quitar una restricción. Obligando al propietario de los datos a pagar un rescate.

Una forma breve de explicar cómo operan estos ciberdelincuentes, es una vez el computador o portátil ha sido infectado con cualquier tipo ransomware, al susceptible usuario le aparecerá una ventana bloqueando el equipo con una dirección de correo o con un mensaje con la cantidad de datos secuestrados. A sabiendas que este será el único método de interactuar usuario y ciberdelincuente, este mensaje lo obliga a recibir instrucciones sobre cómo volver a conseguir el control de sus datos y la máquina. Para poder recuperar la información una solución competentemente fácil es pagar por

el rescate, profesionales en seguridad no avalan estas estas destrezas él no cual no deberíamos de apoyar estas prácticas mal intencionadas. Habitualmente el ciberdelincuente requiere una cantidad de dinero en moneda virtual bitcoins, que al cambio oscila entre los $100 y $1000 dólares norteamericanos, cuando la transferencia del dinero entra en las arcas del delincuente, le hace llegar una clave con la que puede liberar sus datos.

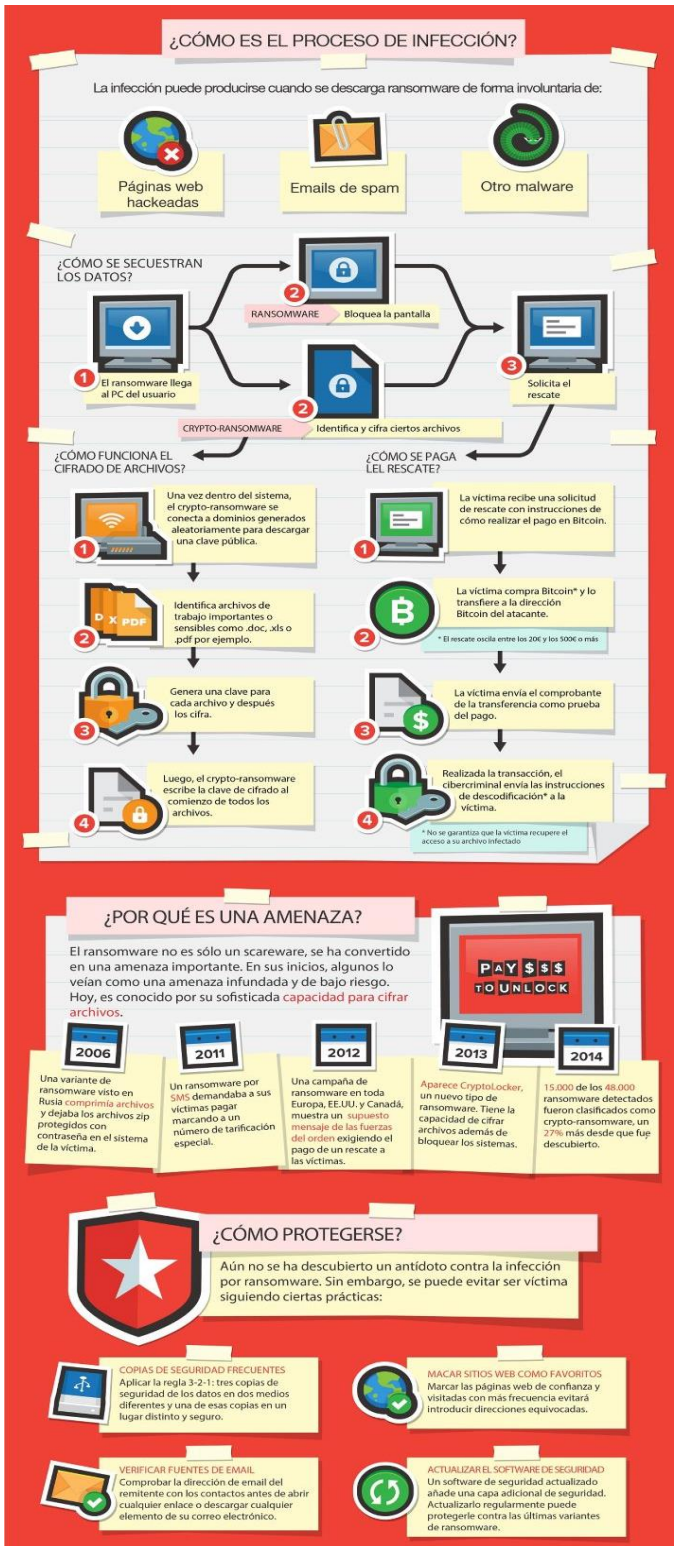

Figura 2: ¿Cómo protegerse? [10].

VIII. ¿QUÉ HACER PARA EVITAR ESTOS ATAQUES?

A pesar que se desarrollan programas para evitar que más personas sean víctimas de estafadores, es importante tener presente algunas recomendaciones que nos trae Sean Williams, director y desarrollador del proyecto Cryptostalker, para detectar ransomware en Windows y Linux:

- Cryptostalker le permite al usuario será capaz de saber si su sistema Linux está infectado con alguna de estas amenazas.
- Security by Default ha desarrollado una aplicación de seguridad llamada AntiRansom especialmente para detectar este tipo de malware en Windows.
- La otra herramienta, CryptoPrevent es una aplicación para Windows diseñada originalmente para prevenir la infección de CryptoLocker, actualmente, proporciona protección contra una amplia gama de ransomware y otros malware.
- Malwarebytes también ha lanzado su herramienta Anti-Ransomware (Beta), capaz de detectar y bloquear CryptoWall4, CryptoLocker, Tesla y CTB-Locker.
- BitDefender también ha lanzado una "vacuna" para protegerse contra versiones de las familias CTB-Locker, Locky y TeslaCrypt: BDAntiRansomware.
- PowerShell y Bash que permite detectar la modificación de ciertos archivos señuelos en el Windows y Linux.

Dentro de otras recomendaciones que todas las personas deberían tener en cuenta:

- Asegurarse de respaldar periódicamente los archivos más importantes.
- La actividad de respaldo debiera ser diversificada, de modo que la falla de un solo punto no provoque la pérdida irreversible de información.
- Almacenar una copia en la nube, en servicios como Dropbox; y las otras en medios físicos fuera de línea, como por ejemplo un disco duro portátil removible.
- Alternar los privilegios de acceso a los datos y fijar permisos de lectura/escritura, de modo que los archivos no puedan ser modificados ni borrados.
- Verificar la integridad de las copias de respaldo de vez en cuando.
- Personalizar los ajustes de anti-spam de la forma correcta.
- La mayoría de las variantes de ransomware son conocidas por difundirse mediante correos que atrapan visualmente y que contienen adjuntos contagiosos. Una gran idea es configurar el servidor de webmail para bloquear adjuntos dudosos con extensiones como .exe, .vbs, .scr. [NT: también, .vbe, ,js, .jse, .bat, .cmd, .dll].
- No abrir adjuntos que parezcan sospechosos.

Adicionalmente, Sean Williams añade que "*la mayoría de las amenazas descritas son capaces de contactar con el servidor de control remoto, es decir, si dispone de acceso a Internet. La idea del desarrollador es trabajar de forma conjunta con otras herramientas existentes y así cerrar el tráfico saliente*

para evitar que el cifrado se complete de forma satisfactoria" [11].

IX. INFORMACIÓN, UNA PUERTA ABIERTA A LA CRIMINALIDAD

La información es un recurso que, como el resto de los activos comerciales, tiene valor para una organización y, por consiguiente, debe ser debidamente protegida; a partir de esta premisa, es indispensable abrir nuevas discusiones desde todas las instancias sobre su manejo y custodia, no solo desde el punto de vista legal, sino también desde la responsabilidad individual para la producción, reciclaje y eliminación de este invaluable bien.

En un mundo en donde "el uso de las tecnologías de la información y las comunicaciones trae consigo cambios y retos permanentes y se constituye como uno de los pilares del mundo globalizado" [13], es de vital importancia darle la preponderancia necesaria, a las nuevas dinámicas que se han generado en torno a lo que, verdaderamente, es la información.

Según la publicación de la plataforma DOMO [2], cada minuto: la web móvil recibe 217 nuevos usuarios, se envían 204.166.667 correos electrónicos, se generan 100.000 tweets en Twitter y son creados 571 nuevos sitios y, precisamente dicha situación, se ha convertido en un bumerang, fenómeno que a diario abre más brechas en el uso de medios tecnológicos con fines delictivos. Es de vital importancia, ahondar sobre los nuevos retos que el mundo de la virtualidad genera, sobre este tema, se podría decir que uno de los primeros pasos en Colombia, es la reciente Ley 1581 de 2012, que hasta el 2013, tímidamente, fue interpretada y aplicada en las diferentes entidades.

Dicha Ley constituye el marco general de la protección de datos personales, y tiene como objeto desarrollar el derecho constitucional (artículo 15 de la Constitución Política de Colombia) que tienen todas las personas a: conocer, actualizar y rectificar las informaciones recopiladas sobre ellas, en pocas palabras los ciudadanos pueden:

- Saber cómo y para qué se usa la información que se brinda a distintas entidades en el país.

- Autorizar, conocer, actualizar y rectificar la información suministrada a las diferentes entidades.

- Evitar que el uso inadecuado de los datos personales afecte la intimidad personal y familiar o que el uso inadvertido de información sensible pueda generar discriminación.

Bajo estos fundamentos, la información esta supuestamente "protegida", pero los colombianos ¿Conocen la Ley?, ¿Custodian los datos registrados en diferentes establecimientos o entidades?, ¿Deciden qué datos pueden ser públicos y cuáles no?; indiscutiblemente el desconocimiento de los derechos es la puerta abierta a la criminalidad.

Lo anterior, se podría decir que el gobierno vela por la información que se encuentra legalmente en manos de terceros, pero existe una vulnerabilidad más alta en aquella que circula o se encuentra almacenada en nuestros propios dispositivos.

Prueba de ello, es uno de los escándalos más recientes, que nuevamente deja la política en el ojo del huracán, en donde Andrés Sepúlveda, fue condenado a 10 años de prisión por los delitos de concierto para delinquir, espionaje, violación de datos personales y uso de software malicioso, luego de ser contratado, supuestamente, por la campaña del partido Centro Democrático, para 'sabotear' el actual proceso de paz.

X. UNA MIRADA A LA CRIMINALIDAD DE LA EMPRESA PRIVADA O PÚBLICA

Indiscutiblemente, lo real de lo virtual es que es un espacio en donde los delincuentes también pueden navegar, aprender de él y usarlo a su favor.

Un ejemplo de esto, es el trabajo que se realiza en tema de seguridad de la información en el Banco Agrario de Colombia, diariamente, esta entidad bancaria contrarresta todo tipo de técnicas enmarcadas en la ingeniería social [3], lo que implica, frecuentemente: actualizar su Política de Seguridad de la Información, capacitar a su personal e informar a los demás miembros de la organización sobre este tipo de ataques, a través de los canales alternos de atención (Banca Virtual, Banca Móvil).

En dicha entidad bancaria, en los últimos meses, uno de los ataques cibernéticos más empleados es conocido como phishing, el cual está enfocado en el conocimiento de los malos hábitos de los usuarios [4], permitiéndoles a los cibercriminales diseñar mejores herramientas, que infecten el equipo del cliente, redirigiendo sus consultas en Internet a páginas fraudulentas (Pharming), donde se captura su información.

Según la Gerencia de Seguridad Bancaria empresas como Incocrédito, Policía de Tránsito Distrital y la franquicia VISA, han sido víctimas de este tipo de ataques, por lo que, en el mes de enero, el Banco Agrario de Colombia, como parte de su estrategia para disminuir el riesgo de Phishing, contrató un servicio para minimizar el riesgo de suplantación de los portales WEB de la Entidad, el cual incluye el monitoreo continuo del sitio web del Banco e identificación y bloqueo de sitios fraudulentos.

Adicionalmente, actualizó el Manual de Procedimientos de Seguridad de la Información, en el cual adicionó un lugar para el registro y atención de este tipo de casos.

XI. LA AMENAZA DE LO INVISIBLE

En ocasiones lo no palpable pone en juego nuestro buen juicio, con esta breve introducción, es de mi menester darle paso a un elemento pasivo en las discusiones de delitos informáticos, por

el hecho que los postulados mencionados anteriormente en este ensayo, se han robado todos los escenarios de discusión, por lo que el uso de dispositivos celulares queda rezagado.
Según el artículo Nuevos Retos, en seguridad informática [12], "se espera que el volumen de aplicaciones maliciosas y de alto riesgo para móviles, crezca hasta 3 millones para finales del 2014", una cifra que al parecer podría estar relacionada con la accesibilidad a la nueva tecnología y, por supuesto, el internet.

Fotos, audios, conversaciones, notas, facturas, claves, contactos, y demás son algunos de los archivos que a diario manejamos a través de estos dispositivos, convirtiéndolos en una máquina de tiempo permanente.

En un artículo de prensa, publicado en el 2012 por el portal www.eset-la.com, durante septiembre fue reportada una grave vulnerabilidad en sistemas operativos Android, que permite al atacante ejecutar remotamente un comando USSD, entre otras cosas, para bloquear la tarjeta SIM o reiniciar el equipo de la víctima a sus configuraciones de fábrica, eliminando en consecuencia de modo permanente toda la información del usuario contenida en el dispositivo.

La vulnerabilidad, que fue presentada en la conferencia de seguridad Ekoparty realizada en Argentina entre el 19 y 21 de septiembre, permite que un atacante ejecute código malicioso en el dispositivo del usuario sin darle la oportunidad de cancelar o detener el ataque una vez que el mismo se inició.

XII. CONCLUSIONES

Ya planteado y desarrollado el problema, podemos concluir que existe una creciente problemática frente al uso de las nuevas tecnologías, un arma de doble filo en desarrollo, que pone en riesgo la privacidad de millones de personas en el mundo.

Sin importar las medidas de seguridad o los programas que desarrollan las grandes compañías de tecnología, siempre existirá una lucha imparable con un enemigo invisible, pero tangible, que sin duda alguna estará a la vanguardia de todas las nuevas tendencias y en la búsqueda de debilidades, que le permitan acceder fácilmente a los archivadores virtuales.

Primero que todo, desde el punto de vista de seguridad personal, es importante que los individuos puedan entrar en contacto y conocer, cuáles son los peligros que acechan el mundo virtual.

El conocimiento es crucial para combatir este tipo de terrorismo, que de forma sigilosa puede entrar a nuestros hogares a través de los celulares, una herramienta que hoy por hoy es crucial para el desarrollo de nuestras actividades.
Es vital que los colegios y las universidades sean involucrados en este proceso, ya que de la capacitación depende el uso responsable de estos medios, a través de medidas preventivas, que cierren poco a poco las brechas ante la inseguridad virtual.
En segunda instancia están las empresas o las organizaciones gubernamentales, las cuales deben blindarse con políticas de seguridad de la información robustas, que impidan la fuga de información a través de cualquier medio.

Gracias al anterior panorama, podemos concluir que sin duda alguna existe un aumento en el volumen de la ciberdelincuencia; adicionalmente, las personas que perpetúan este tipo de actos están lejos de las leyes, leyes que a nivel mundial tienen que efectuarse y cumplirse.

Para combatir futuras intrusiones por los ciberdelincuentes, es necesario blindarnos desde nuestras casas hasta organizaciones privadas y públicas, es, la capacitación y concientización sobre la internet, la informática y las buenas prácticas en el manejo de herramientas tecnológicas. Que nos conllevan a una red segura. Dado a que los problemas de delitos informáticos se están extendiendo de forma exponencial, y mientras los ciberdelincuentes operen libremente a través de las fronteras de la red no habrá quien los detenga.

Finalmente, es crucial que las leyes se ajusten a la realidad, ya que solo así se podrá judicializar este tipo de delitos que también les quita la tranquilidad a las personas, por la vulnerabilidad que esto representa en el quehacer diario.

REFERENCIAS

[1] M. Castells, "Internet y La Sociedad Red" pp. 2 Ponencia, Programa de Doctorado sobre la Sociedad de la Información y el Conocimiento. Universitat Oberta de Catalunya.
[2] El Espectador, "En 2015 aumentaron en 40% los ataques cibernéticos, dice la Policía", 26 de marzo de 2016. Tomado:http://www.elespectador.com/noticias/judicial/2015-aumentaron-40-los-ataques-ciberneticos-dice-polici-articulo-623568
[3] El Tiempo, "Colombia es el tercer país de la región con más ataques cibernéticos", 22 de septiembre de 2015. Tomado: http://www.eltiempo.com/tecnosfera/novedades-tecnologia/ataques-ciberneticos-en-latinoamerica/16383752
[4] Europaprees "El éxito del 'ransomware': cómo se distribuye y qué hacer para prevenirlo". Tomado de: http://www.europapress.es/portaltic/software/noticia-exito-ransomware-distribuye-hacer-prevenirlo-20160709105953.html.
[5] Peter Yeung. "La deep web es mucho más que armas, drogas y sexo", tomado de: http://www.vice.com/es_mx/read/la-deep-web-es-mucho-ms-que-armas-drogas-y-sexo.
[6] Xacata "Una semana en la deep web. Esto es lo que me he encontrado". Tomado de: http://www.xataka.com/analisis/una-semana-en-la-deep-web-esto-es-lo-que-me-he-encontrado.
[7] Omicrono. "Bitcoin: Qué es, cómo funciona y todo lo que necesitas saber". Tomado de: http://www.omicrono.com/2013/04/bitcoin-que-es-como-funciona-y-todo-lo-que-necesitas-saber/.

[8] http://blog.segu-info.com.ar/2016/06/recopilacion-de-todos-los-ransomware-y.html.
[9] A. G. Yuste. "Delitos informáticos: malware, fraudes y estafas a través de la red y cómo prevenirlos", pp 49 – 75. Madrid. 2012.
[10] Trend Micro http://diarioti.com/el-ransomware-en-cifras-y-lo-que-las-organizaciones-deben-saber/98938.
[11] Sean Williams "Recomendaciones para evitar ataques" http://blog.segu-info.com.ar/2016/03/herramientas-para-detectar-ransomware.html.
[12] Compes 3701, Lineamientos de Política para Ciberseguridad y Ciberdefensa