Cibercriminalidad, tendencias de malware y evasión

Sergio Cambra

Universidad Católica Nuestra Señora de la Asunción
Facultad de Ciencias y Tecnología
Ingeniería Informática

Resumen El cibercrimen o la ciberdelincuencia se puede definir como actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos. La cibercriminalidad incluye una amplia variedad de categorías de crímenes. Estas pueden ser clasificadas según la actividad informática, según el instrumento, medio u objetivo y según actividades delictivas graves.

El método más utilizado para la obtención de información o datos personales o bien empresariales, es el phishing empleando técnicas de ingeniería social y algunas veces buscando infectar al usuario con algún tipo de código malicioso. Al conjunto de robots informáticos, es conocido como *botnets* o zombis, en el cual las maquinas son infectadas y manejadas remotamente por un tercero para varios fines.

La cibercriminalidad y el *malware* dirigen su ataque a los sistemas móviles *smartphones* siendo estos dispositivos muy utilizados actualmente. En conclusión tanto los cibercriminales como las entidades de seguridad van aprendiendo y perfeccionando sus métodos para los ataques y las defensas. En definitiva el cibercrimen tendrá una larga vida.

Keywords: cibercrimen, ciberdelincuencia, cibercriminalidad, phishing, botnes, malware

1. Introducción.

La cibercriminalidad constituye uno de los ámbitos delictivos de más rápido crecimiento. Cada vez más delincuentes se aprovechan de la rapidez, la comodidad y el anonimato que ofrecen las tecnologías modernas para llevar a cabo diversos tipos de actividades delictivas. Estas incluyen ataques contra sistemas y datos informáticos, usurpación de la identidad, distribución de imágenes de agresiones sexuales contra menores, estafas relacionadas con las subastas realizadas a través de Internet, intrusión en servicios financieros en línea, difusión de virus, *botnets* (redes de ordenadores infectados controlados por usuarios remotos) y distintos tipos de estafas cometidas por correo electrónico, como el

phishing (adquisición fraudulenta de información personal confidencial).

El alcance mundial de Internet ha permitido a los delincuentes perpetrar casi cualquier actividad ilegal en cualquier lugar del planeta, por lo que todos los países se ven obligados a adaptar sus métodos ordinarios de control a escala nacional para hacer frente a los delitos que se cometen en el ciberespacio. El uso de Internet por los terroristas, en particular para captar adeptos e incitar a la radicalización, representa una grave amenaza para la seguridad tanto a escala nacional como internacional.

2. Cibercriminalidad.

El constante progreso tecnológico que experimenta la sociedad, supone una evolución en las formas de delinquir, dando lugar, tanto a la diversificación de los delitos tradicionales como a la aparición de nuevos actos ilícitos.

Diversos autores y organismos han propuesto definiciones de los delitos informáticos, aportando distintas perspectivas y matices al concepto. Algunos consideran que es innecesario diferenciar los delitos informáticos de los tradicionales, ya que, según éstos se trata de los mismos delitos, cometidos a través de otros medios.

Partiendo de esta compleja situación y tomando como referencia el "Convenio de Ciberdelincuencia del Consejo de Europa", podemos definir los delitos informáticos como: **"los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos"** [1].

Un delito informático es toda aquella acción, típica, antijurídica y culpable, que se da por vías informáticas o que tiene como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet.

Aunque básicamente es cualquier tipo de delito en que el que se utilicen como herramientas ordenadores y se realice a través de redes electrónicas mundiales, el término **CIBERCRIMEN** se encuentra aún en la mesa de debate en cuanto a la legislación de muchos países en el mundo se refiere [2].

3. Clasificación Delitos informáticos.

3.1. Según la Actividad Informática.

- **Sabotaje informático.**
  Comprende todas aquellas conductas dirigidas a causar daños en el hardware o en el software de un sistema. Los métodos utilizados para causar destrozos

en los sistemas informáticos son de índole muy variada y han ido evolucionando hacia técnicas cada vez más sofisticadas y de difícil detección.
Conductas dirigidas a causar daños físicos.
El primer grupo comprende todo tipo de conductas destinadas a la destrucción «física» del hardware y el software de un sistema (por ejemplo: causar incendios o explosiones, introducir piezas de aluminio dentro de la computadora para producir cortocircuitos, echar café o agentes cáusticos en los equipos, etc.
Conductas dirigidas a causar daños lógicos.
El segundo grupo, más específicamente relacionado con la técnica informática, se refiere a las conductas que causan destrozos «lógicos», o sea, todas aquellas conductas que producen, como resultado, la destrucción, ocultación, o alteración de datos contenidos en un sistema informático.

- **Fraude a través de computadoras.**
  Estas conductas consisten en la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias indebidas.

  Los sistemas de comunicación internacional, permiten que una conducta de este tipo sea realizada en un país y tenga efectos en otro.

  Respecto a los objetos sobre los que recae la acción del fraude informático, estos son, generalmente, los datos informáticos relativos a activos o valores. En la mayoría de los casos estos datos representan valores intangibles (ej.: depósitos monetarios, créditos, etc.), en otros casos, los datos que son objeto del fraude, representan objetos corporales (mercadería, dinero en efectivo, etc.) que obtiene el autor mediante la manipulación del sistema. En las manipulaciones referidas a datos que representan objetos corporales, las pérdidas para la víctima son, generalmente, menores ya que están limitadas por la cantidad de objetos disponibles. En cambio, en la manipulación de datos referida a bienes intangibles, el monto del perjuicio no se limita a la cantidad existente sino que, por el contrario, puede ser «creado» por el autor.

- **Copia ilegal de software y espionaje informático.**
  Se engloban las conductas dirigidas a obtener datos, en forma ilegítima, de un sistema de información.

  Es común el apoderamiento de datos de investigaciones, listas de clientes, balances, etc. En muchos casos el objeto del apoderamiento es el mismo programa de computación (software) que suele tener un importante valor económico.

  Infracción de los derechos de autor.
  La interpretación de los conceptos de copia, distribución, cesión y comunicación pública de los programas de ordenador utilizando la red provoca

diferencias de criterio a nivel jurisprudencial.

Infracción del Copyright de bases de datos.
No existe una protección uniforme de las bases de datos en los países que tienen acceso a Internet. El sistema de protección más habitual es el contractual: el propietario del sistema permite que los usuarios hagan *downloads* de los ficheros contenidos en el sistema, pero prohíbe el replicado de la base de datos o la copia masiva de información.

- **Uso ilegítimo de sistemas informáticos ajenos.**
  Esta modalidad consiste en la utilización sin autorización de los ordenadores y los programas de un sistema informático ajeno. Este tipo de conductas es comúnmente cometido por empleados de los sistemas de procesamiento de datos que utilizan los sistemas de las empresas para fines privados y actividades complementarias a su trabajo.

- **Delitos informáticos contra la privacidad.**
  Grupo de conductas que de alguna manera pueden afectar la esfera de privacidad del ciudadano mediante la acumulación, archivo y divulgación indebida de datos contenidos en sistemas informáticos.

  Esta tipificación se refiere a quién, sin estar autorizado, se apodere, 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 cualquier otro tipo de archivo o registro público o privado.

3.2. Según el Instrumento, Medio o Fin u Objeto.

- *Como instrumento o medio.*
  En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

  - Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.)
  - Variación de los activos y pasivos en la situación contable de las empresas.
  - Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)
  - Lectura, sustracción o copiado de información confidencial.
  - Modificación de datos tanto en la entrada como en la salida.
  - Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.
  - Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.

- Uso no autorizado de programas de cómputo.
- Introducción de instrucciones que provocan ïnterrupciones.[en] la lógica interna de los programas.
- Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
- Obtención de información residual impresa en papel luego de la ejecución de trabajos.
- Acceso a áreas informatizadas en forma no autorizada.
- Intervención en las líneas de comunicación de datos o teleproceso.

- *Como fin u objetivo.*
  En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

  - Programación de instrucciones que producen un bloqueo total al sistema.
  - Destrucción de programas por cualquier método.
  - Daño a la memoria.
  - Atentado físico contra la máquina o sus accesorios.
  - Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
  - Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.)

3.3. Según Actividades Delictivas Graves.

Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos:

- *Terrorismo*
  Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional. La existencia de hosts que ocultan la identidad del remitente, convirtiendo el mensaje en anónimo ha podido ser aprovechado por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.

- *Narcotráfico*
  Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.

- *Espionaje*
  El acceso no autorizado a sistemas informáticos gubernamentales e interceptación de correo electrónico del servicio secreto de los Estados Unidos, entre otros actos que podrían ser calificados de espionaje si el destinatario final de esa información fuese un gobierno u organización extranjera.

- *Espionaje industrial*
  También se han dado casos de accesos no autorizados a sistemas informáticos de grandes compañías, usurpando diseños industriales, fórmulas, sistemas de fabricación y *know how* estratégico que posteriormente ha sido aprovechado en empresas competidoras o ha sido objeto de una divulgación no autorizada [3].

4. Delincuencia Financiera.

La delincuencia financiera, también denominada delincuencia de cuello blanco, abarca una amplia gama de delitos, generalmente de ámbito internacional.

Los delitos financieros, estrechamente relacionados con la ciberdelincuencia, se cometen normalmente a través de Internet y tienen una gran repercusión en la banca y la finanza internacional, en su vertiente tanto oficial como alternativa.

Los delitos financieros afectan a particulares, empresas, organizaciones e incluso a Estados, y repercuten negativamente en todo el sistema económico y social debido a las pérdidas considerables de dinero que generan [4].

Ámbitos en la delincuencia financiera:

- *Tarjetas de pago. / Payment cards.*
  Tipos frecuentes de fraude de tarjetas de pago son:
  - *El fraude de aplicación:* un tipo de delito de robo de identidad en el que las tarjetas de pago se obtienen a través de un proceso de solicitud fraudulenta utilizando documentos robados o falsificados.
  - *Toma de control de la cuenta:* otro tipo de delito de robo de identidad, esto suele implicar el engaño de una institución, reedición financiera de una tarjeta de pago y su redirección a una dirección diferente.
  - *Pérdida / Robo de Tarjeta:* como su nombre lo indica, este tipo de fraude consiste en el mal uso de las tarjetas reales que o se pierden o son robados del verdadero titular de la tarjeta.
  - *Tarjeta falsificada:* esto es un fraude realizado con tarjetas de plástico que hayan sido específicamente producidas o tarjetas existentes que han sido alterados. Estas tarjetas están codificados con datos de cuentas de tarjetas de pago obtenidos ilegalmente con el fin de pagar por los bienes y servicios o para retirar dinero en efectivo.
  - *Tarjeta no presente (CNP):* este tipo de fraude se comete utilizando datos de cuentas de tarjetas de crédito para realizar transacciones en las que no hay contacto cara a cara entre el vendedor y el comprador. Normalmente, este tipo de fraude es cometido por Internet, por correo

o por teléfono.

- *Blanqueo de capitales. / Money laundering.*
  La definición de lavado de dinero de INTERPOL es: çualquier acto o intento de ocultar o disfrazar la identidad de los ingresos obtenidos ilegalmente por lo que parece que se originó a partir de fuentes legítimas".
  Fondos ilegalmente obtenidos se lavan y se mueven por todo el mundo usando y abusando de empresas fantasmas, intermediarios y transmisores de dinero. De esta manera, los fondos ilegales permanecen ocultos y son integrados en el negocio jurídico y en la economía legal.

- *Falsificación de moneda y documentos de seguridad. / Counterfeit currency and security documents.*
  El delito de falsificación de moneda es tan antigua como la creación de dinero en sí mismo. La evolución reciente de las tecnologías fotográficas, computadoras e impresión, además de la disponibilidad de equipos de bajo costo, han hecho que la producción de dinero falso sea relativamente fácil.

  Los delincuentes a menudo utilizan documentos de identidad robados o falsos con el fin de llevar a cabo los delitos financieros.

  Se reconoce la necesidad de mejorar la seguridad de los documentos oficiales de dos maneras:
  La mejora de las características de seguridad de los propios documentos oficiales, con el fin de reducir la posibilidad de la falsificación.

  Elevar los estándares de pruebas necesarias para obtener los documentos oficiales. En particular, esto se aplica al registro, certificados de nacimiento del niño y los documentos de viaje de emergencia.

- *Estafa. / Fraud.*
  Los diferentes tipos de fraude incluyen trucos de confianza, el fraude de lotería y el fraude de pago por adelantado, así como el fraude de seguros, la evasión de impuestos, estafas de inversión en el extranjero, fraude de matrimonio, esquemas piramidales y el fraude de tarjetas de pago.

  Estos delitos suelen tener una dimensión internacional y se han comprometido a través de diversos medios de comunicación, por ejemplo a través de Internet, teléfono, fax y correo.

  Sofisticadas técnicas de ingeniería social se llevan a cabo en Internet para engañar a la gente para que revele datos personales, datos bancarios y contraseñas. Una de estas técnicas es el "phishing", en la que los estafadores crean comunicaciones falsas - tales como correos electrónicos, mensajes instantáneos y las ventanas pop-up - que pueden parecer venir de una fuente legítima.

5. Piratería

El término "piratería" abarca la reproducción y distribución de copias de obras protegidas por el derecho de autor, así como su transmisión al público o su puesta a disposición en redes de comunicación en línea, sin la autorización de los propietarios legítimos, cuando dicha autorización resulte necesaria legalmente. La piratería afecta a obras de distintos tipos, como la música, la literatura, el cine, los programas informáticos, los videojuegos, los programas y las señales audiovisuales [5].

Tradicionalmente, la piratería consistía en la reproducción y distribución no autorizadas, a escala comercial o con propósitos comerciales, de ejemplares físicos de obras protegidas. No obstante, el rápido desarrollo de Internet y la utilización masiva en línea, no autorizada, de contenidos protegidos, en la que con frecuencia no existe el elemento "comercial", han suscitado un intenso debate. La cuestión acerca de si dicho uso es un acto de "piratería" y si se debe abordar de la misma manera que la piratería tradicional, constituye el eje del debate actual sobre el derecho de autor. Están surgiendo distintos puntos de vista, a menudo divergentes, y las respuestas a la cuestión difieren de un país a otro. Existen en el mundo diversas formas de piratería y diversos usuarios piratas [6].

En los países de altos ingresos, la conectividad de banda ancha hace que el Internet sea la principal fuente de piratería. Los usuarios pre eren bajar los medios de internet por el hecho de ser gratis y por el hecho de no salir de su hogar y en general se ve que no existe una comprensión clara de la ilegalidad de este hecho (como se vio en el caso del software y de los filmes). En los países de altos ingresos, la piratería digital no comercial ha logrado desplazar casi en su totalidad a la cadena industrial de venta de discos pirateados. Parte de la razón de este cambio se debe al enfoque de sitios Web como *BitTorrent* y otros servicios de intercambio entre usuarios (P2P). En este contexto, los tribunales se han mostrado receptivos hacia el alegato de la industria sobre la responsabilidad civil por daños a terceros, aun cuando esos sitios Web no son más que motores de búsqueda.

6. Phishing.

Phishing es un término informático que denomina un tipo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El cibercriminal, conocido como *phisher*, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas. [7]

La mayoría de los métodos de *phishing* utilizan la manipulación en el diseño del correo electrónico para lograr que un enlace parezca una ruta legítima de la organización por la cual se hace pasar el impostor. URLs manipuladas, o el uso de subdominios, son trucos comúnmente usados por *phishers*.

En otro método popular de *phishing*, el atacante utiliza contra la víctima el propio código de programa del banco o servicio por el cual se hace pasar. Este tipo de ataque resulta particularmente problemático, ya que dirige al usuario a iniciar sesión en la propia página del banco o servicio, donde la URL y los certificados de seguridad parecen correctos. En este método de ataque (conocido como *Cross Site Scripting*) los usuarios reciben un mensaje diciendo que tienen que verificar sus cuentas, seguido por un enlace que parece la página web auténtica; en realidad, el enlace está modificado para realizar este ataque, además es muy difícil de detectar si no se tienen los conocimientos necesarios.

El *phishing* es un mecanismo que se viene utilizando hace mucho tiempo para robar información personal y financiera empleando técnicas de ingeniería social y algunas veces buscando infectar al usuario con algún tipo de código malicioso. Para entender mejor el informe publicado por el APWG (*Anti-Phishing Working Group*) una campaña de *phishing* corresponde a un único correo electrónico enviado a múltiples usuarios, dirigiéndolos a un sitio web falso específico, aunque múltiples campañas pueden dirigir a un mismo sitio.

Sobre el conteo de campañas únicas a partir del campo de asunto del correo electrónico, el APWG toma los siguientes datos donde se puede ver que durante el primer trimestre de este año la cantidad de campañas tuvo un comportamiento decreciente:

De enero a marzo de este año la cantidad de casos únicos de *phishing* reportados descendió un 31 %. Además, estos valores comparados con el último trimestre del 2012 muestran un descenso del 20 %. Del punto de vista mensual, el máximo valor registrado en este trimestre es 28850, que es un 29 % menos que el mayor histórico de 40621 reportados durante agosto de 2009.

Este decrecimiento, de acuerdo al informe es el reflejo de que los ciberdelincuente están utilizando los servidores que comprometen no para los ataques de *phishing*, sino más bien para más malware o ataques de denegación de servicio, además estos cambios probablemente se deban a un cambio de las técnicas para el robo de credenciales hacia unas más avanzadas y específicas que incluyen *malware*.

A pesar que se ve una disminución durante el primer trimestre, con estos valores los niveles en la cantidad de casos de *phishing* se pone a la par de los valores record que se presentaron en 2012.

Figura 1. Cantidad de campañas de Phishing.

Figura 2. Cantidad de sitios web de Phishing.

En el informe también resalta el hecho de que la mayoría de sitios de *phishing* están alojados en servidores web que han sido comprometidos. Si bien Estados Unidos, por ser el país con mayor cantidad de dominios web en el mundo, sigue siendo el país con mayor cantidad de sitios relacionados con casos de *phishing*, países como Canadá experimentaron un crecimiento en la cantidad de detecciones de este tipo de sitios. De acuerdo al informe este cambio muestra el cambio en los patrones de propagación de este tipo de campañas. [8]

A partir de los datos de este informe, se puede ver una disminución en la cantidad de campañas y sitios web que utilizan el phishing para robar información del usuario, lo cual no significa por ningún motivo que los peligros sean menos. Como bien resalta el informe, las amenazas pueden estar migrando hacia otras un poco más avanzadas pero con el mismo objetivo: obtener datos sensibles, para luego llevar a cabo algún tipo de fraude.

7. Botnets.

Botnet es un término que hace referencia a un conjunto de robots informáticos o *bots*, que se ejecutan de manera autónoma y automática. El artífice de la *botnet* puede controlar todos los ordenadores/servidores infectados de forma remota y normalmente lo hace a través del IRC (*Internet Relay Chat*). Las nuevas versiones de estas *botnets* se están enfocando hacia entornos de control mediante HTTP, con lo que el control de estas máquinas será mucho más simple. [9]

Debido a que un equipo infectado por *bots* cumple las órdenes de su amo, muchas personas se refieren a estos equipos víctima como "zombis". Los delincuentes cibernéticos que controlan estos *bots* son cada vez más numerosos.

Algunos *botnets* pueden englobar cientos o un par de miles de equipos, pero otros cuentan con decenas e incluso centenares de miles de zombis a su servicio. Muchos de estos equipos se infectan sin que sus dueños se enteren. ¿Existe algún indicio? Un *bot* puede hacer que su equipo funcione más lento, muestre mensajes misteriosos e, incluso, falle.

7.1. Cómo funcionan los bots.

Los *bots* se introducen sigilosamente en el equipo de una persona de muchas maneras. Los *bots* suelen propagarse por Internet en busca de equipos vulnerables y desprotegidos a los que puedan infectar. Cuando encuentran un equipo sin protección, lo infectan rápidamente e informan a su creador. Su objetivo es permanecer ocultos hasta que se les indique que realicen una tarea [10].

Una vez que un *bot* toma el control de un equipo, se puede utilizar para realizar varias tareas automatizadas, como las siguientes:

- *Enviar:* spam, virus, software espía.

- *Robar:* roban información privada y personal y se la comunican al usuario malicioso; datos como, números de tarjeta de crédito, credenciales bancarias, otra información personal y confidencial.

- *DoS (denegación de servicio):* Lanzan ataques de denegación de servicio (DoS) contra un objetivo específico. Los criminales cibernéticos extorsionan a los propietarios de los sitios web por dinero, a cambio de devolverles el control de los sitios afectados.

- *Fraude mediante clics:* Los estafadores utilizan *bots* para aumentar la facturación de la publicidad web al hacer clic en la publicidad de Internet de manera automática.

7.2. Ejemplo: Usando una Botnet para enviar Spam.

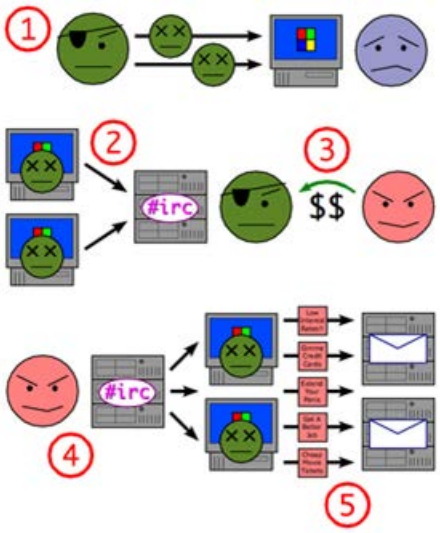

Figura 3. Usando una Botnet para enviar Spam [10].

- Paso 1. El operador de la botnet manda virus/gusanos/etc a los usuarios.
- Paso 2. Los PC entran en el IRC o se usa otro medio de comunicación.
- Paso 3. El Spammer le compra acceso al operador de la Botnet.
- Paso 4. El Spammer manda instrucciones vía un servidor de IRC u otro canal a los PC infectados.
- Paso 5. Causando que éstos envíen Spam a los servidores de correo.

8. Tendencias de ciberdelincuencia para el 2013.

Una tendencia al alza de la ciberdelincuencia que se está dando en todas las regiones del mundo con un altísimo coste como una de las principales consecuencias. [11]

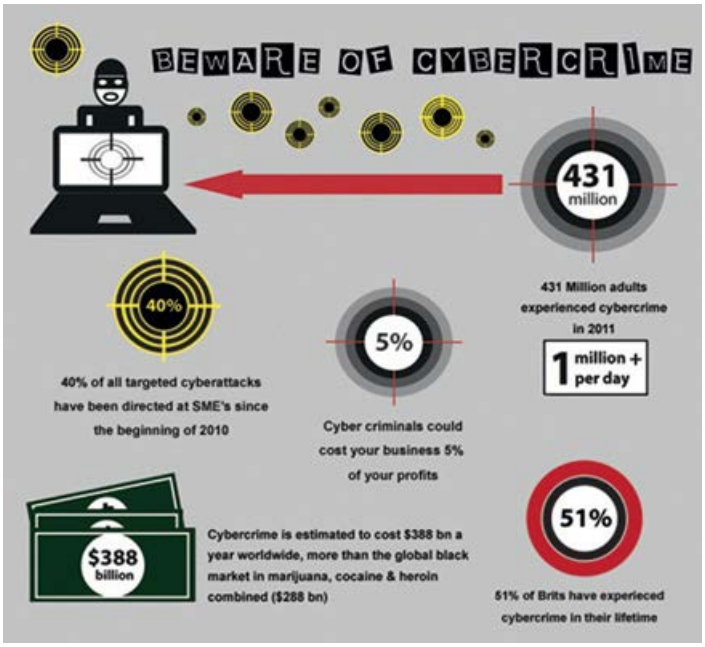

Figura 4. Cuidado con el cibercrimen.

Figura 5. Principales amenazas cibernéticas para las empresas.

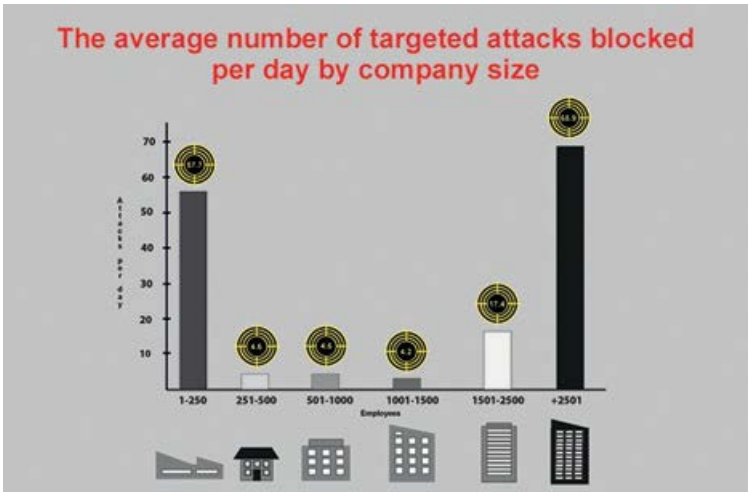

Figura 6. Número medio de ataques dirigidos bloqueados por día por tamaño de empresa.

9. Estadísticas y tendencias del cibercrimen.

Más de 550 millones de personas son víctimas del cibercrimen al año, una cifra que bien puede ser unificada a las que ya se muestran en la entrada Tendencias de ciberdelincuencia para 2013 y a las 600.000 cuentas que diariamente quedan comprometidas en Facebook, aunque el móvil principal de los ciberataques es hacer daño a la industria objetivo.

En esta infografía se puede ver las tendencias que se esperan hasta 2017, cuando el mercado de seguridad pase a ganar 120 billones (de mil millones) de dólares de los 63 que ganó en 2011 y la actividad del cibercrimen cause un daño de 100.000 millones de dólares. [12]

Figura 7. Estadísticas sobre cibercriminalidad.

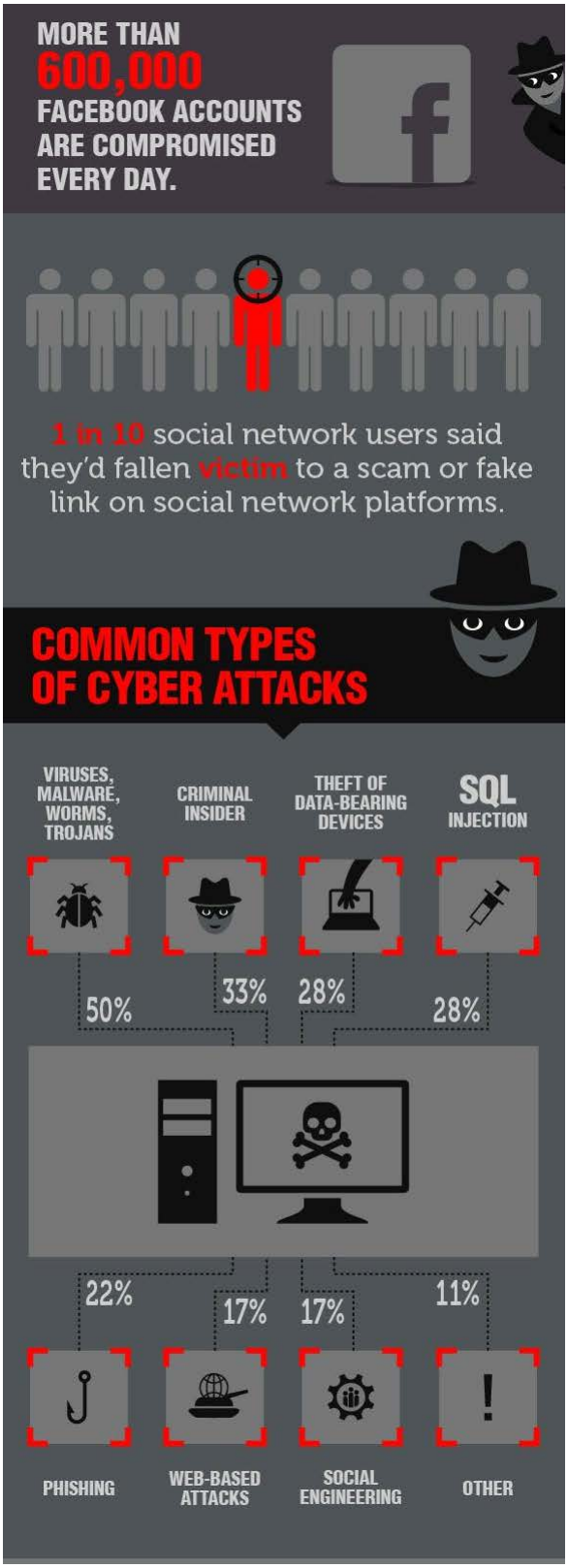

Figura 8. Tendencias de ataques.

10. Los cibercriminales se sirven de la nube para camuflar malware.

La descarga dinámica del *malware* alojado en la nube ofrece nuevas posibilidades a la industria del cibercrimen.

Expertos de **G Data SecurityLabs** han constatado la consolidación de una nueva tendencia del cibercrimen: el *malware* desde la nube, o lo que es lo mismo, ciberciminales que usan tecnología *cloud* para camuflar sus ataques. En una reciente campaña de *malware* detectada por G Data, el fabricante alemán pudo comprobar por primera vez el uso de la nube para camuflar *malware* del tipo *infomation stealer*, un tipo de amenaza que, por ejemplo, incluye programas espías o troyanos bancarios. Esta técnica les permite, por ejemplo, alojar las funciones maliciosas de sus troyanos bancarios en la nube, dificultando la detección y la toma de contramedidas. Las soluciones de seguridad de G Data, equipadas con la tecnología proactiva *G Data BankGuard*, protegen frente a esta nueva amenaza bancaria.

Troyanos bancarios.
Los troyanos bancarios se sirven, de forma habitual, de archivos de configuración almacenados en el ordenador de la víctima. Estos archivos contienen el código malicioso que, mediante un ataque de inyección, añaden en las direcciones web que visita la víctima con el objetivo de interceptar la comunicación usuario - banco. Dicho código es el responsable del robo de los datos.

Nuevo camuflaje Cloud.
Con esta nueva funcionalidad, parte de esos archivos de configuración del troyano, se trasladan a la nube. De esta forma, los creadores de malware dificultan los análisis de soluciones antivirus y las propias medidas de seguridad adoptadas por la banca. [14]

Figura 9. Ataque clásico "Man in the Browser".

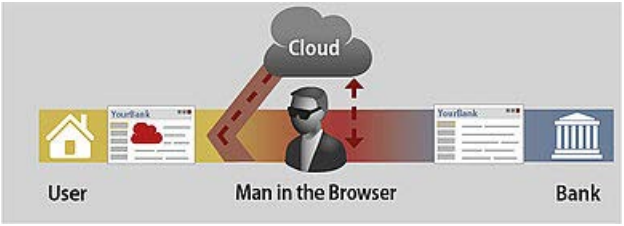

Figura 10. Robo de información aprovechando tecnología Cloud.

11. Tendencias de malware.

Debido al aumento en ventas de *smartphones* con Android y iOS, la variación en el tipo de uso aplicado a estos dispositivos, y considerando la rápida evolución que ha tenido esta tecnología y los códigos maliciosos para móviles en el 2012, es posible establecer como principal tendencia para 2013, un crecimiento exponencial de *malware mobile* como también, una mayor complejidad de éstos ampliándose así el rango de acciones maliciosas que realizan en el dispositivo.

Otro hito que se podrá observar en 2013 es la consolidación de un cambio de paradigma que se viene gestando en los últimos años. Se trata del modo en cómo los códigos maliciosos son propagados por los cibercriminales y los medios que utilizan para ese fin. En ese sentido, la propagación de malware a través de dispositivos de almacenamiento extraíbles está disminuyendo para dar paso al uso de un intermediario con el objetivo de obtener nuevas víctimas. Un intermediario es un servidor web comprometido por un tercero con el fin de alojar amenazas informáticas. Posteriormente, los ciberdelincuentes proceden a enviar hipervínculos que dirigen al usuario hacia el código malicioso en cuestión. A su vez, parte de esta metodología es que toda la información robada es almacenada en estos servidores vulnerados para evitar involucrar computadoras personales.

11.1. Aumento de malware para móviles.

A partir de 2010, los códigos maliciosos para dispositivos móviles así como dicho mercado, empezaron a experimentar grandes cambios que marcarían la historia posterior de este tipo de amenazas. En primer lugar, Android comenzó a posicionarse como el sistema operativo *mobile* más utilizado dentro de la competencia. Por otra parte, en ese mismo año, *FakePlayer* se convertía en el primer código malicioso diseñado para la plataforma de Google.

Un año después, la creación de códigos maliciosos y variantes para Android no solo aumentaron considerablemente sino que también la complejidad de estos ataques, el tiempo y recursos que destinan los ciberdelincuentes en el desarrollo de *malware* para *mobile*. Resulta lógico que un sistema operativo móvil con

una tasa de participación de mercado del 65.9 % sea tan apetecible para los ciberdelincuentes, pues tienen mayor probabilidad de obtener ganancias ilícitas en comparación con otro cuya cantidad de usuarios, sea inferior.

En la siguiente tabla se muestra la tasa de participación de los principales sistemas operativos móviles que existen en la actualidad:

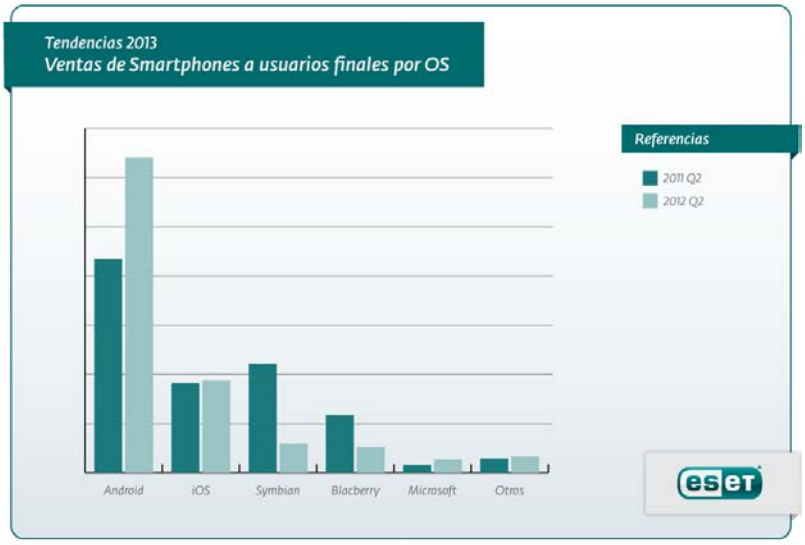

Figura 11. Ventas de SMARTPHONES a usuarios finales por OS. [15]

A medida que la cuota de mercado de Android crezca y los usuarios lo utilicen cada vez más para almacenar información personal y corporativa, realizar transacciones bancarias, o consultar cualquier otro servicio similar, los cibercriminales desarrollaran más *malware* para cumplir el objetivo de robar información y de ese modo, obtener ganancias ilícitas. En base a esto y al igual que los códigos maliciosos diseñados para computadores, el principal motivo e interés de los ciberdelincuentes por crear este tipo de amenazas sigue siendo la obtención de dinero.

De acuerdo a una encuesta realizada por ESET Latinoamérica sobre el uso que le dan los usuarios a los dispositivos móviles, se pudo determinar que aunque el almacenamiento de información privada y contraseñas no es la tarea que más realizan las personas por el momento, sí posee un porcentaje bastante considerable. A continuación, se muestra el grafico con las estadísticas al respecto:

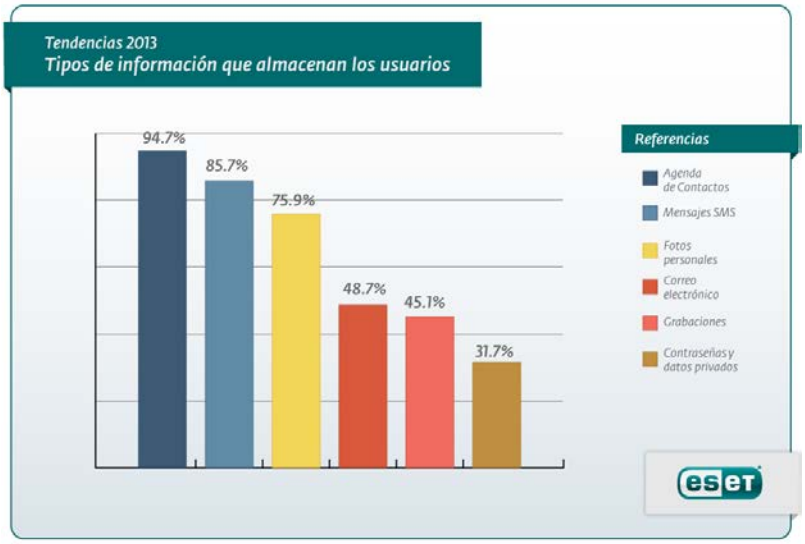

Figura 12. Tipo de información que almacenan los usuarios en dispositivos móviles.

La información más utilizada por los usuarios en estos dispositivos es la agenda de contactos. En base a esto, existen códigos maliciosos pata Android diseñados con el fin de robar este tipo de datos. Esto le resulta útil a los ciberdelincuentes para poder obtener nuevas víctimas. Las contraseñas e información privada ocupan un 31.7 % de las preferencias, evolucionando tecnológicamente, y los servicios se adapten a esta tendencia desarrollando aplicaciones y sitios web optimizados específicamente para *Smartphone*.

11.2. Troyanos SMS.

Con respecto al tipo de código malicioso más común para dispositivos Android, y considerando que los mayores aumentos en el número de variantes fueron protagonizados por dos amenazas de este tipo, se destacan los troyanos SMS. Durante 2012, de la totalidad de reportes de detecciones únicas de *malware* desarrollados para el sistema operativo de Google, el troyano *Android/TrojanSMS.Boxer.AQ* encabeza la lista. Luego, le sigue *Android/Plankton.H* y *Android/TrojanSMS.Agent.BY.GEN*. En la siguiente página, se muestra una infografía que explica el funcionamiento general de este tipo de código malicioso para móviles:

Figura 13. Funcionamiento de troyanos SMS.

Mientras este tipo de negocio fraudulento siga siendo rentable y fácil de implementar por parte de los ciberdelincuentes, es probable que los troyanos SMS sigan siendo la categoría de amenaza móvil más común durante 2013.

11.3. Propagación de malware vía sitios web.

Con la introducción de la primera versión comercial de *Windows XP* en 2001, y la masificación de los dispositivos de almacenamiento extraíbles (*pendrive*), se comenzó a gestar una era marcada por los gusanos que se propagan a través de estos medios aprovechándose de una vulnerabilidad de diseño del *Windows XP* (*Autorn*). Gracias a que este problema fue solucionado en 2009, y que los usuarios han migrado hacia versiones de *Microsoft Windows*, la cantidad de códigos maliciosos que continúan utilizando esta técnica han ido disminuyendo en los últimos años.

De hecho, en el trascurso de 2012 aquellas detecciones relacionadas con esta vulnerabilidad de diseño (INR/Autorun y otras) han ido decreciendo sostenidamente. Por otro lado, detecciones genéricas como *HTML/Scrinject.B*, *HTML/lframe* y *JS/TrojanDownloader.lframe.NKE* comenzaron a ocupar el segundo lugar y otros puestos respectivamente. Todas esas firmas tienen como objetivo detectar diversos sitios web que han sido comprometidos y modificados por un atacante para propagar *malware*. En la mayoría de los casos, son paginas legitimas que pertenecen a empresas de diversos rubros y que, producto de alguna vulnerabilidad, protección insuficiente, o configuración inadecuada, han sido modificadas por un ciberdelincuente que ha logrado obtener acceso al servidor en donde se encuentran alojadas. Posteriormente, los cibercriminales proceden a inyectar scripts maliciosos o etiquetas lframe que redirigen al usuario hacia la descarga de alguna amenaza. En algunos casos la información que roban también la suben a este servidor comprometido con el fin de evitar utilizar computadoras personales y de ese modo, dificultar la identificación de estos individuos.

En la siguiente tabla se pueden observar los crecimientos porcentuales que han experimentado durante 2011 y 2012, algunas firmas genéricas utilizadas para detectar códigos maliciosos que se propagan a través de dispositivos de almacenamiento extraíbles y sitios web comprometidos.

A continuación, se presenta un gráfico que comprende todo 2011 hasta setiembre de 2012 en lo que respecta al porcentaje de detecciones asociadas a gusanos *Autorun* y amenazas que son propagadas a través de un servidor web vulnerado.

Como puede observarse, a principios de 2011 las firmas relacionadas a sitios web comprometidos eran prácticamente nulas. Conforme fue avanzando el año pasado, la detección *Autorun* comenzó a disminuir hasta que en setiembre de 2011, fue superada por las detecciones tipo HTML. Asimismo, tanto HTML como JS han ido experimentando un crecimiento considerable a través del tiempo.

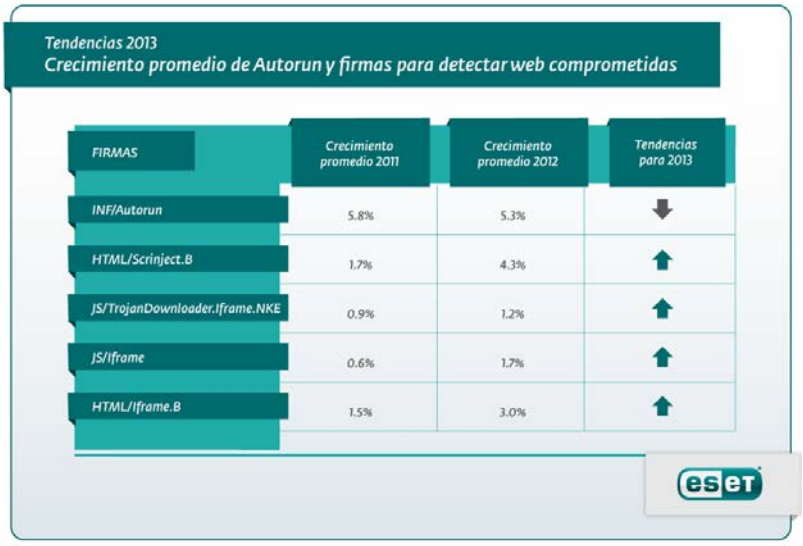

Figura 14. Crecimiento promedio de Autorun y firmas para detectar web comprometidas 2011 vs 2012.

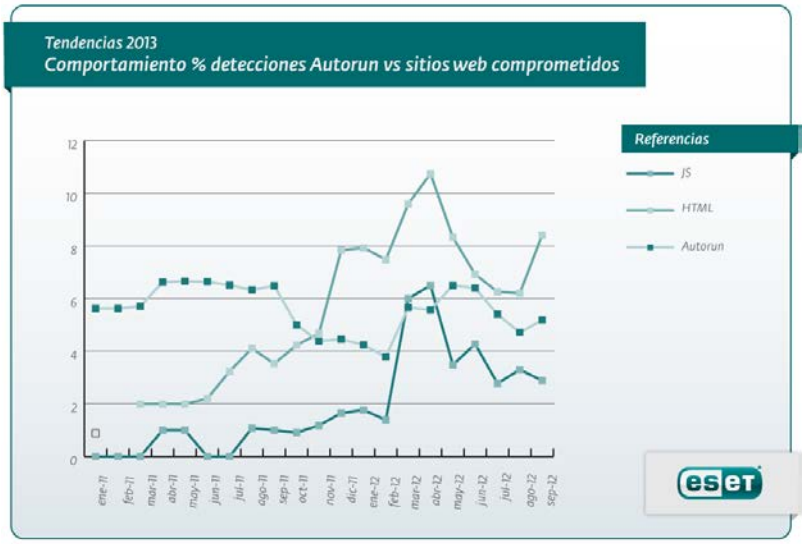

Figura 15. Comportamiento porcentual de detecciones Autorun vs sitios web comprometidos.

Esto permite establecer como tendencia, un aumento sostenido en el uso de esta técnica para infectar potenciales víctimas y por ende, un decrecimiento en el uso de gusanos que se aprovechan de los dispositivos de almacenamiento extraíbles con este fin.

Antes de esta tendencia de cambio en los métodos de propagación de códigos maliciosos, los cibercriminales propagaban directamente el *malware* a través de algún medio (correo, redes sociales, recursos corporativos, dispositivos de almacenamiento extraíble, entre otros) hacia la computadora de la víctima tal como puede apreciarse en el siguiente esquema:

Figura 16. Correo electrónico, chat, dispositivos USB, redes sociales, sitios web maliciosos. Métodos tradicionales de propagación de malware.

Con este nuevo paradigma de distribución de *malware* utilizando sitios web comprometidos, los cibercriminales recurren a un intermediario (servidor comprometido) para infectar a las victimas puede verse a continuación:

Figura 17. Malware, Bornets, Phishing. Propagación utilizando un intermediario.

Para que esta situación de propagación vía sitios web ocurra, los cibercriminales recurren a las siguientes etapas:

- El ciberdelincuente explota una vulnerabilidad presente en un servidor web. Allí modifica el sitio original para poder inyectar código malicioso.
- Comienza a propagar el enlace que dirige hacia la amenaza alojada en el servidor comprometido, redes sociales, o cualquier medio que le sirva para dicho fin.

- El usuario visita este sitio y descarga el malware. En algunos casos, la información que se le roba a la víctima también es almacenada en ese intermediario.

Antes de esta tendencia, los cibercriminales omitían todo este proceso y propagaban el código malicioso directamente hacia las potenciales víctimas. Asimismo, la información que robaban era almacenada en sus propias computadoras.

Por otro lado, sumada esta nueva técnica de propagación también puede considerar la táctica *Black Hat SEO*. [16] Mediante esta técnica, los cibercriminales posicionan ilícitamente los sitios web maliciosos dentro de los primeros resultados de una búsqueda realizada en un buscador. Por lo general utilizan palabras clases relacionadas a tragedias o temas de interés masivo, para que las potenciales víctimas sientan curiosidad y visiten dichas páginas con facilidad. Finalmente, es importante destacar que los ataques de phishing suelen ser desplegados a través de un intermediario como también, aquellos centros de comando y control (C&C) pertenecientes a una red *botnet*.

12. Evasión de malware.

El ingenio del *malware* no se limita a su funcionalidad o su capacidad para propagarse. A veces, el código malicioso tiene que tener la astucia para sobrevivir.

Eso significa que en mayor parte tiene una comprensión innata de cuando está siendo analizada por un experto en seguridad. Numerosas muestras de diferentes familias de *malware* han demostrado maneras hábiles para evadir la detección, por ejemplo, denegar la ejecución si detecta que está siendo abierto dentro de una máquina virtual, o si una conexión de protocolo de escritorio remoto se usa para mirar el código. Otros serán dormir durante un período de tiempo definido antes de la ejecución, a la espera tal vez para detectar los movimientos del ratón para asegurarse de que un ser humano está en la rueda, y no un escáner de código automatizado.

La supervivencia es de suma importancia, en particular para los ataques dirigidos que cualquier combinación de *malware* nuevo o viejo está en juego. Para el investigador, mantenerse a la vanguardia del juego significa mejoras constantes a las artes de análisis, tales como *sandboxes*. *The sandbox* puede ser personalizado para extraer configuraciones en busca de *malware*, desde troyanos bancarios a *botnets* o *malware* utilizados en ataques dirigidos.

Una ocurrencia que está ayudando a los investigadores en su lucha contra el malware de detección de *Sandbox* es la disponibilidad del código fuente de *Citadel*. El troyano bancario conocido surgió después de que el código fuente del

troyano Zeus se filtró en 2011, y emplea varias tácticas de evasión incluyendo la capacidad de detectar los archivos y procesos utilizados por el *software* de virtualización, hacer comparaciones con perfiles conocidos de *sandbox* en línea, como *Anubis*, o dormir hasta que el reconocimiento de lo que interpreta como movimientos humanos. Una vez más, en un estilo clásico del gato y el ratón, ambos lados del pasillo están aprendiendo. [**?**]

13. Conclusión.

Si uno intenta bloquear un camino de hormigas con una piedra, éstas muy pronto encuentran una vía alternativa para seguir con sus actividades.

Con esta frase concluyo el trabajo de investigación, la cibercriminalidad está en un nuevo auge, los smartphones, y si vuelve a aparecer una nueva tecnología o dispositivo, estén seguros que la creatividad o la necesidad harán frente a las nuevas tendencias y se encontrara la manera de realizar estos crímenes informáticos.

Referencias

1. Consejo de Europa: Convenio sobre la ciberdelincuencia. http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/consejo_europa/convenios/common/pdfs/Convenio_Ciberdelincuencia.pdf
2. Delito informático: http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico
3. *Delitos informáticos* http://www.monografias.com/trabajos6/delin/delin.shtml
4. INTERPOL: Cibercriminaldad http://www.interpol.int/es/Criminalidad/Delincuencia-financiera/Delincuencia-financiera
5. *Pirata informático* http://es.wikipedia.org/wiki/Pirata_inform%C3%A1tico
6. Observatorio Mundial de Lucha Contra la Piratería. http://portal.unesco.org/culture/es/ev.php-URL_ID=39397&URL_DO=DO_TOPIC&URL_SECTION=201.html
7. Phishing. http://es.wikipedia.org/wiki/Phishing
8. Phishing Activity Trends Report. http://docs.apwg.org/reports/apwg_trends_report_q1_2013.pdf
9. Botnet. http://es.wikipedia.org/wiki/Botnet
10. Bots y botnets: Una amenaza creciente. http://mx.norton.com/botnet
11. *Infografía: Tendencias ciberdelincuencia 2013.* http://itercriminisblog.com/index.php/tendencias-ciberdelincuencia-2013/
12. *Infografía: Estadísticas y tendencias del cibercrimen.* http://itercriminisblog.com/index.php/estadisticas-y-tendencias-del-cibercrimen-infografia/
13. Tendencias 2013: Malware en móviles http://www.eset-la.com/pdf/prensa/informe/tendencias_2013_vertiginoso_crecimiento_malware_moviles.pdf
14. Banking Trojans disguise attack targets in the Cloud. http://blog.gdatasoftware.com/blog/article/banking-trojans-disguise-attack-targets-in-the-cloud.html
15. Gartner Report. http://www.gartner.com/newsroom/id/2120015
16. Ataques BlackHat SEO. http://blogs.eset-la.com/laboratorio/2010/07/05/ataques-blackhat-seo/