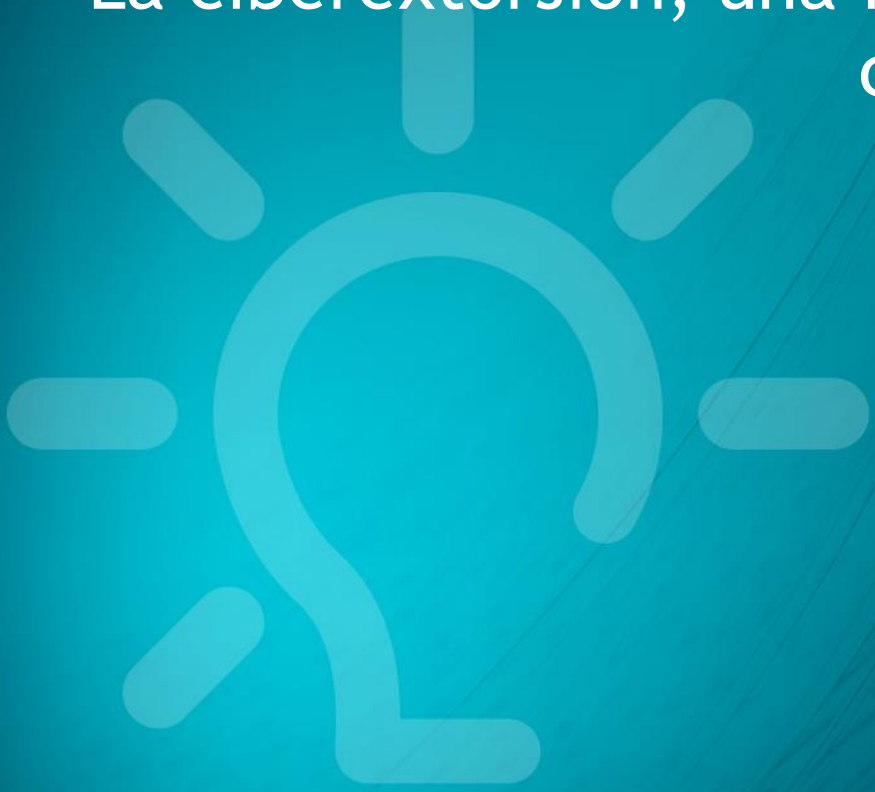
CyberThreats_
Telefónica

La ciberextorsión, una industria en crecimiento

22/02/2016



Telefónica

securely powered by
ElevenPaths

Principales descubrimientos

Existe una creciente tendencia a la agresión en numerosos ataques cibernéticos, en particular en aquellos que utilizan algún método de extorsión. En este sentido, las conclusiones sobre los métodos llevados a cabo que están teniendo un mayor impacto son los siguientes:

- La extorsión a través de **ataques DDoS** se está estableciendo sólidamente. El *modus operandi* del grupo DD4BC podría dar lugar a que más atacantes pudieran hacerse pasar por ellos sin necesidad de una gran infraestructura y conocimientos técnicos amplios. Por otro lado, se ha identificado que una de las posibles salidas de dinero con el objetivo de blanqueo retornado a raíz de las extorsiones son las plataformas de juego *online* y de *trading*.
- Las **brechas de seguridad** están suponiendo una vía de extorsión en función de la sensibilidad de la información filtrada. Actualmente, para monetizar los ataques se está optando por dos vías, o bien poner a la venta la base de datos o bien extorsionar directamente a los usuarios. El medio de pago solicitado suele ser Bitcoin.
- Una tendencia cada vez mayor es la **extorsión sexual**, también conocida como *sextorsion*. El intercambio de archivos en redes *peer-to-peer* sigue siendo la principal plataforma para el acceso a material de abuso infantil y para su distribución de forma no comercial. De la misma manera, plataformas como Tor y otras redes anónimas son consideradas como una amenaza en esta área. Sin embargo, lo que más preocupa a las Fuerzas y Cuerpos de Seguridad es la transmisión en vivo de maltrato infantil debido a la dificultad para detectarlo e investigarlo ya que los delincuentes no suelen almacenar una copia del material.
- Desde 2015, la amenaza de ***ransomware*** se ha visto incrementada en un 165%. El vector de infección más reportado es el correo electrónico con archivos adjuntos maliciosos. Sin embargo, se espera un crecimiento motivado por el aumento del uso del *cloud*, POS y el internet de las cosas.

El uso de las *criptodivisas*, así como de Tor y de las redes P2P son los elementos comunes a los diferentes tipos de extorsión y seguirán siendo las principales amenazas mientras que no existan soluciones lo suficientemente potentes para su monitorización.

Tabla de contenidos

Introducción

Los delitos informáticos son cada vez más hostiles. Existe una creciente tendencia a la agresión en muchos de los ataques cibernéticos y, en particular, en aquellos en los que se emplea alguna modalidad de extorsión. Estos ataques tienen cierto impacto psicológico con el objetivo de inducir el miedo e incertidumbre en sus víctimas, acercándose más a un ambiente de delincuencia organizada que a un delito informático al uso.

De esta manera, las Fuerzas y Cuerpos de Seguridad se enfrentan ante ciertos desafíos en la fase de investigación para la aplicación de la ley. Muchas operaciones suelen acabar frustradas debido a la utilización de herramientas para la anonimización y el cifrado de las comunicaciones por parte de los criminales. El conocimiento de seguridad en las operaciones es elevado y el fácil acceso que poseen los ciberdelincuentes a productos y servicios fácilmente accesibles en internet, tanto para anonimizar su actividad como su identidad, suele complicar los análisis forenses realizados.

En este sentido, el informe tiene el objetivo de identificar las principales técnicas empleadas con un mayor impacto en ataques de DDoS, robo de información confidencial, extorsión sexual y *ransomware* con el fin de informar sobre cuáles son las limitaciones técnicas a las que se enfrenta el investigador ante la realización de posibles ejercicios de atribución en la red.

Modalidades de extorsión

La extorsión se puede definir como el acto de obtener la propiedad o dinero de otro con la amenaza de emplear cualquier tipo de fuerza. Asimismo, las amenazas en la red que se valen de la técnica de la extorsión son las siguientes:

Ataques de Denegación de Servicio Distribuido (DDoS)

Los informes realizados por la industria de seguridad consideran los ataques de DDoS como amenazas con grandes repercusiones. Esta amenaza consiste en un tipo de ataque contra una red de equipos causando que un servicio o recurso sea inaccesible a los usuarios legítimos. En 2015, aunque varios ataques superaron los 100 Gigabits por segundo, otros de menor magnitud causaron también importantes problemas de disponibilidad. De hecho, las tres cuartas partes de los ataques suelen durar menos de cuatro horas, lo que sugiere que se trata de un tiempo más que suficiente para que un atacante logre su objetivo (1).

La extorsión a través de este vector de ataque se está estableciendo sólidamente. Uno de los grupos que más repercusión han logrado ha sido DD4BC (DDoS para Bitcoin). Sus primeros ataques se registraron a finales de 2014 y sus rescates oscilan entre 1 y 100 bitcoins dependiendo de la situación financiera percibida de la víctima y su voluntad para seguir las instrucciones. Con el propósito de aumentar la credibilidad de su amenaza, el grupo suele lanzar un pequeño ataque contra la infraestructura de la víctima y trata de comunicarse periódicamente con ella exigiéndole un mayor rescate. En la Tabla I, se pueden observar los procedimientos más comunes para ponerse en contacto con sus víctimas.

DD4BC se dirige principalmente a la industria del juego en línea, pero recientemente ha ampliado su actividad y está dirigiendo sus ataques también a empresas del sector financiero (Anexo A). Por otro lado, no es tan claro que todos los ataques puedan ser atribuidos a un solo grupo criminal o hasta qué punto otros delincuentes están tratando replicar su modelo de negocio utilizando su nombre.

Tabla I. Ubicación de perfiles de DD4BC.

Nombre de perfil	Plataforma	URL	Dirección de alta
dd4bc	Klout	http://www.klout.com/dd4bc	
	Twitter	http://twitter.com/dd4bc	bo********@t*****.***
	Bitcointalk	https://bitcointalk.org/index.php?action=profile;user=dd4bc	
	Instagram	http://www.instagram.com/dd4bc	d****9@hotmail.com
	Disqus	https://disqus.com/dd4bc	
	Bitcointa	http://bitcointa.lk/members/?username=dd4bc	
	Ebay	http://www.ebay.com/usr/dd4bc	
	Slideshare	http://www.slideshare.net/dd4bc	
	Fanbitcoin	http://fanbitcoin.com/index.php?action=profile;user=dd4bc	
dd4bcddos	Skype		
ddd4bc	Skype		dd4bc@outlook.com
dd4bc1	Skype		
	Bitmessage[1]	BM-NC1jRewNdHxX3jHrufjxDsRWXGdNisY5	

Por el momento, no ha sido posible verificar si se trata de un único grupo o de más que han ido replicando su modus operandi. De todas formas, a medida que la reputación de DD4BC y sus diferentes modus operandi vayan conociendo, podría llegar a convertirse en un fenómeno en el que los atacantes pudieran hacerse pasar por este grupo sin necesidad de una gran infraestructura y conocimientos técnicos amplios.

Key Threat: criptodivisas como medio de pago

Bitcoin es la criptodivisa por excelencia utilizada por DD4BC para recibir los rescates. Mientras que el uso lógico suele ser el empleo de una dirección de Bitcoin por rescate con el fin de dificultar el seguimiento de las transacciones, este grupo suele utilizar las mismas direcciones para diferentes extorsiones. Incluso llegando a aparecer direcciones de los presuntos atacantes entre las que deberían ser direcciones de una presunta víctima. Además, las cantidades recibidas por las direcciones registradas como atacantes son demasiado bajas. Estos indicios introducen la posibilidad de que se estén generando escenarios ficticios para hacer creer a sus víctimas que verdaderamente existen pagos hacia sus direcciones. Si esta hipótesis fuera correcta,

[1] Bitmessage es un protocolo de comunicaciones P2P utilizado para enviar mensajes cifrados a otra persona o para muchos suscriptores.

los atacantes simplemente tendrían que lanzar el ataque mientras que tienen disponibles una serie de correos electrónicos o perfiles abiertos con el fin de contactar con la víctima y haber realizado una serie de operaciones básicas de Bitcoin para crear un escenario creíble. Ambas acciones requieren un coste y un tiempo mínimo de planificación.

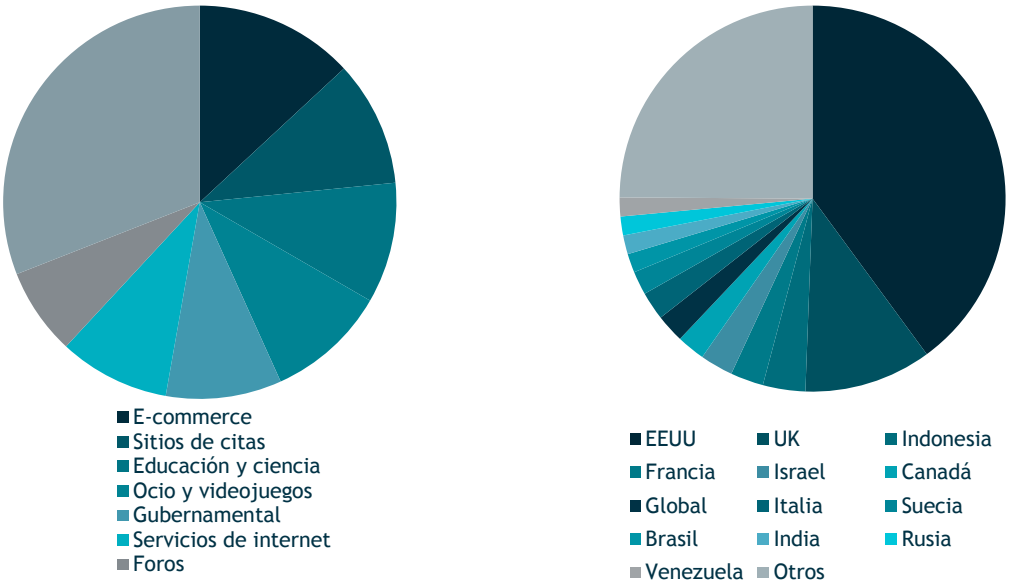
De la misma manera, las direcciones asociadas a DD4BC han emitido bitcoins hacia dos tipos de plataformas: de juego *online* y de *trading*. La primera, a cambio de un coste asumible para hacer la apuesta podría llegarse a multiplicar las ganancias, en cambio, las plataformas de trading estarían orientadas a hacer depósitos de dinero durante un tiempo determinado con réditos exageradamente elevados. Ambos métodos permitirían además de duplicar las ganancias derivadas de la extorsión a difuminar el rastro ya que solamente este tipo de plataformas *online* serían las que tuvieran la información sobre las direcciones utilizadas por cada usuario.

Robo de información confidencial

En diciembre de 2013 se produjo una de las mayores brechas de seguridad con la filtración de información personal de más de 70 millones de clientes de la empresa norteamericana Target (2), un incidente que motivó la movilización inmediata de recursos en ciberseguridad por valor de hasta cinco millones de dólares (3). Aunque las empresas son cada vez más conscientes de la necesidad de securizar sus activos tecnológicos, el año 2015 ha estado marcado por una gran cantidad de brechas de seguridad que ha supuesto una amenaza tanto para usuarios como empresas, independientemente del país y del sector al que pertenezcan (4).

Aunque las motivaciones que subyacen de una filtración pueden tener diversos objetivos, el principal es el de rentabilizar la información sustraída, en gran medida poniéndola a la venta en el mercado negro o a través de campañas de extorsión hacia los usuarios afectados. En mayo y julio de 2015, Adult Friend Finder y Ashley Madison vieron filtrados los datos personales y sensibles de millones de sus clientes, exponiendo a sus usuarios a posibles extorsiones (5) dada la naturaleza de la información filtrada.

Tabla II. Número de ataques por sector (izq.) y país (dch.).



Key Threat: naturaleza de la información filtrada

Este tipo de filtraciones cobran especial relevancia en el caso de que se tenga acceso a las contraseñas en claro, ya que si el usuario empleara la misma o una deducible a partir de ella existiría un gran riesgo de accesos no autorizados. Normalmente, este no es el caso dado que lo habitual es almacenar un resumen o *hash* de la misma. Sin embargo, si la contraseña es poco robusta podrían emplearse técnicas de *cracking* y recuperar la contraseña original. Aun en el escenario más inofensivo, el atacante tendría una cuenta de correo válida que podría utilizar para llevar a cabo ataques de *spam* o de ingeniería social, además de conocer el consumo de un servicio por parte del usuario.

Key Threat: redes anónimas y mecanismos de pago anónimos

Una vez que se tiene acceso a la información de los usuarios, el atacante suele optar por dos vías en función de la sensibilidad de la información, o bien poner a la venta la base de datos íntegra como pasó con Adult Friend Finder (6) a través de foros de Tor, o bien extorsionar directamente a los usuarios como ocurrió con Ashley Madison (7). En ambos casos, el medio de pago que se solicitaba era Bitcoin.

Extorsión sexual o *sextorsion*

Una tendencia cada vez mayor es la extorsión sexual, también conocida como *sextorsion*. Entendemos este tipo de extorsión como la situación que se produce cuando una persona es coaccionada con una imagen o vídeo de sí misma desnuda o realizando actos sexuales que previamente ha sido compartida.

El modus operandi suele iniciarse con un contacto inicial a través de plataformas sociales. Dada la gran cantidad de menores que utilizan este tipo de plataformas, los atacantes tratan de buscar aquellos más propensos a responder de forma favorable (8). Por otro lado, también se han visto otras técnicas más sofisticadas en las que ciertas víctimas fueron instigadas a descargarse *software* malicioso (9) para captar imágenes de los menores y obligarlos a los a continuar con el abuso físico de forma offline.

Otros muchos casos de extorsión son una consecuencia del *sexting*. *Sexting* se define como el intercambio de mensajes e imágenes sexuales, normalmente autogenerada, enviadas a través del teléfono móvil o internet (10). La tecnología existente puede facilitar una difusión no deseada de las imágenes a terceros, que afecta al bienestar de su autor, y que puede derivar en acoso o intimidación, tanto *online* u *offline*, con consecuencias dramáticas que han terminado con el suicidio de los afectados en algunos casos.

Key Threat: plataformas peer-to-peer y redes anónimas

El intercambio de archivos en redes *peer-to-peer* sigue siendo la principal plataforma para el acceso a material de abuso infantil y para su distribución de forma no comercial. Esta tecnología se percibe por los atacantes como fácil de usar ya que el contenido puede ser identificado a través de herramientas de búsqueda. Europol ya en 2015, llegó a identificar un traspaso de atacantes desde redes anónimas a redes *peer-to-peer* (11).

A pesar de ello, plataformas como Tor y otras redes anónimas también son consideradas como una amenaza en esta área, ya que están siendo utilizadas por los atacantes para facilitar el intercambio de imágenes o vídeos de una forma difícil de rastrear. Según Europol, también estas redes estarían siendo utilizadas para compartir guías sobre cómo eliminar cualquier rastro que pudiera identificar a los autores o cómo incluir detalles en el fondo de las imágenes para introducir ruido de cara a los investigadores (12). De la misma manera, recientes desarrollos de Tor incluyen tanto la posibilidad de descarga de aplicaciones móviles en dispositivos

Android así como *hardware* destinado a anonimizar el tráfico, lo que podría motivar un aumento de su utilización.

También se han producido intercambios de material de abuso infantil a cambio de bitcoins a través de Tor Mail. Aunque muchos de los atacantes no intercambian este tipo de contenido con objetivos económicos, Tor y Bitcoin crean el escenario ideal para añadir una variable económica al intercambio tradicional.

En cualquier caso, no se observa un uso creciente de Tor sino también del uso de sistemas de cifrado, como TrueCrypt, o la utilización de VPN, correos electrónicos desechables, *proxies* o conexiones a internet a través de redes wifi abiertas.

Key Threat: live streaming

La popularización de las cámaras web y plataformas de chat que permiten la transmisión de vídeo es lo que está llevando a su explotación por parte de los abusadores sexuales de niños. Algunas de las aplicaciones permitirían a cambio de una cuota emisiones protegidas por contraseñas proporcionándoles una capa extra de anonimato. La transmisión en vivo de maltrato infantil es probable que se vea incrementada debido a las dificultades que conllevan su detección y posterior investigación ya que los delincuentes no suelen almacenar una copia del material.

Key Threat: distribución comercial

Según las Fuerzas y Cuerpos de Seguridad existe la necesidad de comprender el actual alcance de los tipos de distribución de material de abuso infantil a través de la red. Existen, además del método tradicional de distribución en sitios web dedicados, nuevos métodos como los "sitios web disfrazados", los *cyberlockers*[2], la transmisión en vivo mediante pago, así como instancias comerciales en redes anónimas (13). Además, también se ha observado una migración de los mecanismos de pago tradicionales a otros que ofrecen mayor grado de anonimato como Bitcoin.

Ransomware

Este método de extorsión se trata de un tipo de malware que impide o limita a los usuarios a acceder a su información al haber sido cifrada mediante técnicas que no permiten la recuperación de la información a no ser que el ciberdelincuente nos facilite las contraseñas para descifrar los archivos. De esta manera, obliga a sus víctimas a pagar un rescate a través de ciertos métodos de pago *online* con el fin de

[2] Los *cyberlockers* son servicios diseñados específicamente para alojar contenido estático, mayormente archivos grandes.

poder recuperar sus sistemas o sus datos de nuevo (14). A principios de 2015, empresas como McAfee han visto incrementar un 165% sus detecciones respecto a esta amenaza (15). Asimismo, sus características han evolucionado en complejidad. Cada vez es más frecuente encontrar comunicaciones más seguras, técnicas de lanzamiento encubiertas y una mayor conciencia sobre los ambientes de las *sandbox* (16).

Key Threat: vectores de infección más frecuentes

La práctica de infección más utilizado por los delincuentes es la distribución de *malware* mediante correos electrónicos con archivos adjuntos maliciosos. Al mismo tiempo, la utilización de *exploit kits* alojados en páginas web que explotan vulnerabilidades de Flash, Internet Explorer, Silverlight y Java es cada vez más común. Asimismo, los métodos utilizados por los atacantes para atraer a las víctimas están basados en los resultados obtenidos a través de los motores de búsqueda a partir de términos potencialmente ilícitos o embarazosos.

Key Threat: mecanismos de pago más utilizados

Después de pedir inicialmente los pagos de las recompensas con tarjeta de crédito, se adoptó el sistema de pagos rápidos, aunque varía en función de la infección regional del *ransomware*. Este sistema fue implantado hasta que ha sido reemplazado por el uso de las *criptodivisas* combinadas con el uso de Tor para la anonimización total del rastro. Esta tendencia se debe principalmente a un mayor conocimiento sobre los usos que pueden darse a las monedas digitales.

Key Threat: aparición de nuevas formas de ransomware

Son diferentes los tipos de *ransomware* que están siendo detectados y que pueden convertirse en una tendencia. En función del activo afectado se pueden clasificar como sigue:

- *RansomWeb*

Los primeros casos descubiertos de *ransomware* para aprovecharse de las vulnerabilidades de los servidores web podrían ser un indicio sobre una tendencia de futuro. La técnica RansomWeb se dio a conocer a principios de 2015 cuando una empresa de servicios financieros llevó a cabo el rescate por 50 000 dólares de una de sus bases de datos, una cifra que iba aumentando un 10% con cada semana que pasaba (17). A pesar de ello, se ha podido comprobar que los ataques más efectivos

son los que se están efectuando sobre pymes con rescates que rondan los 1000 dólares.

- *Ransomware-as-a-Service*

Mientras que la industrialización del *Crimeware-as-a-Service* no es nueva, la distribución de *ransomware* se revela particularmente innovadora con su estrategia de negocio criminal. En mayo del año 2015, McAfee descubrió un kit llamado 'Tox' disponible de forma gratuita en Tor con el fin de adquirir una participación del 30% de Bitcoins sobre los rescates realizados (18). El código base de Tox carecía de la complejidad de las otras variantes cripto-*ransomware*. Sin embargo, es probable que este modelo de negocio se desarrolle al ofrecer *malware* más avanzado a criminales menos técnicos.

- *Mobile ransomware*

Los ataques de *ransomware* a dispositivos móviles son cada vez más frecuentes. En este sentido, el *malware* Trojan-Ransom registró la tasa de crecimiento más alta de todas las amenazas móviles. Según Kaspersky Lab, el número de nuevas muestras detectadas en Q1 de 2015 fue de 1113, lo que supuso un incremento del 65% en el número de muestras ransomware móvil (19).

- *Cloud, Point of Sale and Internet of Things*

Posiblemente el uso generalizado de dispositivos inteligentes y el creciente uso del *cloud* incentiven el uso de métodos sencillos para la obtención de beneficios económicos a través de infecciones de *malware*. Por otro lado, también es posible la evolución en un refinamiento de los métodos de exfiltración de datos de tarjetas de crédito a partir de terminales de punto de venta (POS) en particular en períodos en lo que existan picos de ventas.

Puntos comunes entre tipos de extorsión

Debido a las características de las monedas virtuales éstas se están convirtiendo en un mecanismo de pago comúnmente utilizado entre los cibercriminales. Con el fin de minimizar esta tendencia, las *criptomonedas* lentamente van ganando aceptación entre los gobiernos europeos ya sea proponiendo a la Unión Europea una regulación (20) o reconociéndolos bajo la legislación de los Estados Miembro (21). Lo cierto es que cualquier regulación de *criptomonedas* tal y como están concebidas hoy probablemente sea solo aplicable a usuarios identificables que hagan uso de pasarelas de intercambio, ya que son estas las que poseen información sobre actividades y cuentas asociadas a cada uno de sus usuarios. La incapacidad de realizar ejercicios de atribución por parte de los investigadores sobre las transacciones realizadas hace que sea difícil imaginar cómo cualquier regulación podría aplicarse en la práctica a usuarios que utilizaran este tipo de monedas diariamente.

Las opciones de comunicación utilizadas por los delincuentes difieren considerablemente. Siguen siendo el correo electrónico, las salas de chat o los IRC los métodos de comunicación más comunes, ubicados tanto en la *surface* como en la *deep web*. Para la comunicación en tiempo real se emplea con cierta regularidad Jabber e ICQ.

Asimismo, según las Fuerzas y Cuerpos de Seguridad de los países de la Unión Europea aseguran que en más de las tres cuartas partes de las investigaciones se encontraron con el uso de algún sistema de cifrado con el fin de proteger la información y/o frustrar el análisis forense de los medios incautados. De la misma manera, también se ha observado un incremento de uso de correo electrónico cifrado.

Por último, cualquier cibercriminal que pretenda mantener un mínimo de seguridad operacional tiene al alcance soluciones de anonimización, como el uso de *proxies* y redes VPN, además del crecimiento de la adopción de Tor e I2P como soluciones alternativas.

Recomendaciones

Vista la amenaza de los diferentes tipos de extorsión en la red, se proponen una serie de recomendaciones para los diferentes proveedores de seguridad con el fin de reducir las limitaciones técnicas existentes en los ejercicios de atribución ante extorsiones en la red:

- Existe margen de mejora en la creación de soluciones para la investigación y monitorización de pagos de *criptodivisas* y en el descubrimiento de usuarios en redes anónimas. Actualmente, las soluciones de las que se disponen son limitadas para la realización de ejercicios de atribución.
- En muchas ocasiones, la solución para la detección de delitos en internet pasa por la creación unidades de fuentes humanas motivado por las limitaciones técnicas existentes y la necesidad de crear ciertos vínculos con el atacante con el fin de obtener información adicional y que van más allá de los procesos automáticos de recolección.
- Existe una necesidad de una legislación común respecto a las *criptodivisas* que permita a las Fuerzas y Cuerpos de Seguridad solicitar la información necesaria a las plataformas de intercambio de divisas existentes en internet de forma ágil.
- Es necesaria la creación de comunidades destinadas a compartir el conocimiento existente en Big Data y en métodos utilizados para la realización eficiente de los ejercicios de atribución en la red, así como para su relación con otros casos anteriores.

Anexos

Relación de ataques identificados de DD4BC

Fecha	Email	Víctima	Dirección de Bitcoin	Precio
23/09/2014		Nitrogen Sports	17WQov8BTXJAemWmqn5XJ8ibiq13SNoaqs	
oct-14		Cex.io		2 BTC
oct-14	dd4bc@outlook.com	Coinsweeper	16JEzTkXGeCFPrCoPo9hnSVZWLHMau31fg	2 BTC
23/10/2014	dd4bc@outlook.com	bitsquare.io		2 BTC
28/10/2014	dd4bc@outlook.com	Mmpool.org	17aLGgw8AwJdqiBtMMG1QtQJgNQQkiyEsp	
29/10/2014		SocialCex.com		
nov-14		blisterpool.com	17aLGgw8AwJdqiBtMMG1QtQJgNQQkiyEsp	2 BTC
02/11/2014	anonymousemail@anonymousemail.us	nicehash.com	16JEzTkXGeCFPrCoPo9hnSVZWLHMau31fg	1 BTC
03/11/2014	dd4bc@outlook.com	bitalo.com	17aLGgw8AwJdqiBtMMG1QtQJgNQQkiyEsp	1 BTC
07/11/2014	dd4bc@outlook.com	bitbillions.com	17aLGgw8AwJdqiBtMMG1QtQJgNQQkiyEsp	1 BTC
15/11/2014	dd4bc@outlook.com	mpex.co	132EdUarcghK2barhkxgaKQ2XqnchPbWSB	1 BTC
17/11/2014	dd4bc@unseen.is	ruggedinbox.com	1MRFFgSexGzyWgbLEhX1Bi3YXR6FaaebV8	1 BTC
ene-15		Betbtc.com		
22/01/2015		Hivewallet.com		
03/02/2015		Exco.in		
15/02/2015	dd4bc@safe-mail.net	Bitquick.com	1HpFnMfz6iDBbckWFMVvKR8mfTteXKHWZc	1.5 BTC
15/02/2015	dd4bc@Safe-mail.net	Holytransaction.com	1E8R3cgnr2UcusyZ9k5KUvkj3fXYd9oWW6	1.5 BTC
mar-15		Antpool		
mar-15		Bitmain		
mar-15		Bw.com		
mar-15		Ckpool		3 BTC
mar-15		Ghash.io		
mar-15		HashNest		
01/04/2015		Neteller		
05/04/2015		betatcasino.com	1NbhLM43duL2J2tBX2qQWBojEm5fNSoMEp	10 BTC
05/04/2015		betatcasino.com		
05/04/2015		slottyvegas.com	1NbhLM43duL2J2tBX2qQWBojEm5fNSoMEp	10 BTC
05/04/2015		Slottyvegas.com		
09/04/2015		Redbet.com		
09/04/2015	dd4bct@gmail.com		18NeYaX6GCnibNkwyuGhGLuU2tYzbxvW7z	20 BTC
10/04/2015		Pokerstars.com		
19/04/2015			15QMfpfymmkgj1AtEy9uvqvpgsTfDuGzJF	15 BTC
may-15		Expresscoin.com		
21/06/2015	dd4bcteam@keemail.me		1KU3TFMNxmE5UTMsjBmep34K6QJtJNJ6wD	25 BTC
		Nitrogen Sports	1H2bstU3yCpqJyrNzHSrnperZnTMSwLa5K	
			198QaeuJ6oMeuan2p5gyDx75odweMWzNXH	

Bibliografía

1. **Securelist.** Kaspersky DDoS Intelligence Report Q2 2015. [Online] 4 agosto 2015. [Cited: 15 febrero 2016.] https://securelist.com/analysis/quarterly-malware-reports/71663/kaspersky-ddos-intelligence-report-q2-2015/.

2. **Target.** Target Provides Update on Data Breach and Financial Performance. [Online] 10 enero 2014. [Cited: 21 diciembre 2015.] https://corporate.target.com/press/releases/2014/01/target-provides-update-on-data-breach-and-financia.

3. —. Target Invests $5 Million in Cybersecurity Coalition. [Online] 18 febrero 2014. [Cited: 21 diciembre 2015.] https://corporate.target.com/article/2014/02/target-to-invest-5-million-in-cybersecurity-coalit.

4. **Telefónica.** *2015: The Year of Information Leaks.* 2015.

5. **SC Magazine UK.** Possible Ashley Madison extortion campaign identified. [Online] 23 octubre 2015. [Cited: 9 febrero 2016.] http://www.scmagazineuk.com/possible-ashley-madison-extortion-campaign-identified/article/448993/.

6. **The Hacker News.** Hackers Selling Database of 4 Million Adult Friend Finder Users at $16,800. [Online] 25 mayo 2015. [Cited: 9 febrero 2016.] http://thehackernews.com/2015/05/AdultFriendFinder-database.html.

7. **ZDNet.** In Ashley Madison's wake, here's one man's story of sex, sorrow and extortion. [Online] 24 septiembre 2015. [Cited: 9 febrero 2016.] http://www.zdnet.com/article/in-ashley-madisons-wake-heres-one-mans-story-of-sex-sorrow-and-extortion/.

8. *Study facilitating the identification, description and evaluation of the effects of new information technologies on the abuse and exploitation of children.* **Oficina de las Naciones Unidas contra la Droga y el Delito.**

9. **FBI.** Cyber Alerts for Parents & Kids. [Online] https://www.fbi.gov/news/stories/2012/february/sextortion_021012.

10. *A qualitative study of children, young people and sexting.* **Science, The London School of Economics and Political.**

11. *The Internet Organised Crime Threat Assessment (IOCTA).* **Europol.** 2015.

12. *The Internet Organised Crime Threat Assessment (iOCTA).* **Europol.** 2014.

13. *Internet Watch Fundation Annual and Charity Report 2013.* **IWF.** 2013.

14. **Trend Micro USA.** Ransomware. [Online] [Cited: 9 febrero 2016.] http://www.trendmicro.com/vinfo/us/security/definition/Ransomware.

15. *Threats Report May 2015.* **McAfee.** 2015.

16. **Telefónica.** Ransomware. [Online] 6 julio 2015. [Cited: 9 febrero 2016.]

17. **Forbes.** RansomWeb: Crooks Start Encrypting Websites And Demanding Thousands Of Dollars From Businesses. [Online] 28 enero 2015. [Cited: 11 febrero 2016.] http://www.forbes.com/sites/thomasbrewster/2015/01/28/ransomweb-50000-dollar-extortion/#3f1541bd7d47.

18. **Security Affairs.** Tox, how to create your ransomware in 3 steps. [Online] 26 mayo 2015. [Cited: 12 febrero 2016.] http://securityaffairs.co/wordpress/37180/cyber-crime/tox-ransomware-builder.html.

19. **Securelist.** IT threat evolution in Q1 2015. [Online] 6 mayo 2015. [Cited: 12 febrero 2016.] https://securelist.com/analysis/quarterly-malware-reports/69872/it-threat-evolution-in-q1-2015/.

20. **hipertextual.com.** Europa quiere terminar con el anonimato del Bitcoin. [Online] 3 febrero 2016. [Cited: 15 febrero 2016.] http://hipertextual.com/2016/02/anonimato-del-bitcoin.

21. **RT News.** Germany recognizes Bitcoin as 'private money'. [Online] 18 agosto 2013. [Cited: 15 febrero 2016.] https://www.rt.com/news/bitcoin-germany-recognize-currency-641/.