BITCOIN Y MALWARE. ¿UN NUEVO MODELO DE NEGOCIO?

MISTIC: MÁSTER UNIVERSITARIO CONJUNTO EN SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Memoria de la tésis de Master de los estudios del master universitario conjunto en seguridad de las tecnologías de la información y las comunicaciones, presentado por Joel Sevilleja Febrer y dirigido por Cristina Pérez Solá.

Universitat Oberta de Catalunya, 2013

A Esther, mi novia, por su paciencia cuando no he tenido tiempo para ella.
A los errantes y a Ernesto, por las muestras de malware.
A mis compañeros de trabajo, por aguantarme mientras les
preguntaba día sí y día también,
¿Alguien sabe algo de Bitcoins?
A mis padres, por su apoyo incondicional.
Y a Cristina, por sus correciones, consejos e interés.

Resumen

El presente documento pretende analizar el malware que está surgiendo en torno a Bitcoin. En primer lugar, se ha realizado un breve análisis de Bitcoin, su funcionamiento y los distintos métodos legítimos para obtenerlos. A continuación, se han repasado brevemente los distintos métodos para obtener beneficios de la industria del cibercrimen. Una vez conocida la metodología que se emplea, se han obtenido muestras de malware y ha creado un pequeño laboratorio para analizarlas. Por último, se ha comparado la rentabilidad de este tipo de malware con los métodos legítimos de obtención de Bitcoin.

Palabras clave

Bitcoin, malware, moneda digital, cibercrimen, minado

Índice general

1. Introducción **3**
- 1.1. Objetivos . . . 4
- 1.2. Metodología . . . 4
- 1.3. Planificación . . . 5

2. Estado del arte **7**
- 2.1. Conceptos básicos . . . 7
- 2.2. Casas de cambio . . . 10
  - 2.2.1. Funcionamiento . . . 11
  - 2.2.2. Comparativa . . . 12
  - 2.2.3. Anonimicidad y casas de cambio . . . 13
  - 2.2.4. Ataques a las casas de cambio . . . 13
- 2.3. Minado de Bitcoins . . . 14
  - 2.3.1. Análisis de los dispositivos de minado . . . 16
- 2.4. Cibercrimen . . . 20
  - 2.4.1. Phishing . . . 21
  - 2.4.2. Troyanos . . . 21
  - 2.4.3. Ransomware . . . 22
  - 2.4.4. Exploit Kits . . . 22

3. Configuración del laboratorio **24**

4. Ataques a Bitcoin **26**
- 4.1. Malware . . . 26
  - 4.1.1. Malware distribuido a través de Skype . . . 26
  - 4.1.2. Skynet . . . 29
- 4.2. Phishing . . . 32
- 4.3. Ransomware . . . 33
- 4.4. Ataques dirigidos . . . 33
  - 4.4.1. Ataques de minado . . . 33
  - 4.4.2. Robo de bitcoins . . . 34
- 4.5. Minado desde aplicaciones legítimas . . . 34
  - 4.5.1. Cliente de ESEA . . . 34
  - 4.5.2. MyFreeProxy . . . 35
- 4.6. Ataques al diseño de Bitcoin . . . 35

5. Conclusiones **37**

Referencias **39**

A. Hardware para el minado de Bitcoins **42**
- A.1. ASIC . . . 43
- A.2. FPGA . . . 44
- A.3. Tarjetas Gráficas . . . 45
  - A.3.1. ATI AMD . . . 45
  - A.3.2. Nvidia . . . 55
- A.4. CPUs/APUs . . . 60

A.4.1. ARM 60
A.4.2. AMD 60
A.4.3. Intel 61
A.4.4. Otros 64

B. Otras monedas **65**
B.1. Litecoin 65
B.2. Namecoin 65

Glosario **68**

Índice de figuras

1.1. Planificación del proyecto 5

2.1. Transiciones en la red Bitcoin 7
2.2. Formación de la cadena de bloques en Bitcoin 8
2.3. Ramas simultáneas en la red Bitcoin. La más larga es la aceptada. 8
2.4. Estructura de un *pool* de minado 9
2.5. Variación del precio del Bitcoin en dólares en MtGox 10
2.6. Variación del precio del Bitcoin en dólares en Bitcoin Exchange 10
2.7. Variación del precio del Bitcoin en dólares en BitStamp 11
2.8. Dispositivos de minado de Butterfly Labs 14
2.9. Captura de pantalla del "Virus de la Policía" 22

3.1. Un sistema Alix 24
3.2. Formulario de Cuckoo Sandbox 25

4.1. Número de visitas recibidas desde bit.ly 26
4.2. Número de visitas recibidas desde goo.gl 27
4.3. Peticiones de bit.ly por país 27
4.4. Peticiones de goo.gl por país 27
4.5. Análisis realizado con *Virus Total* el día de su descubrimiento. 28
4.6. Análisis realizado con *Virus Total* el pasado mes de diciembre 28
4.7. Comunicación del software de minado con el servidor del Pool 29
4.8. Ruta almacenada en una muestra de Kelihos, hacia el fichero *wallet.dat* 29
4.9. Captura del panel de control del proxy de minado de bitcoins 31
4.10. Resultados de la búsqueda de totalhash 31
4.11. Captura de pantalla de una web de phishing centrada en MtGOX. 32
4.12. Captura de pantalla del ransomware Reveton. 33

Índice de tablas

2.1. Dispositivos PCI . . . 12
2.2. Perdidas de BTC más significativas hasta el momento en sitios webs. . . . 13
2.3. Dispositivos PCI . . . 14
2.4. Dispositivos externos . . . 15
2.5. Chips especializados . . . 15
2.6. Servicios en la nube de mercurybtc. . . . 15
2.7. Dispositivos PCI. Beneficios brutos para un periodo determinado, expresado en dólares. . . . 17
2.8. Dispositivos PCI. Beneficios netos para un periodo de tiempo determinado, expresado en dólares. . . . 17
2.9. Dispositivos Externos. Beneficios brutos para un periodo de tiempo determinado, expresado en dólares. . . . 17
2.10. Dispositivos Externos. Beneficios netos obtenidos para un periodo de tiempo determinado, expresado en dólares. . . . 18
2.11. Dispositivos en la nube. Beneficios netos obtenidos a 1 año vista, expresado en dólares. . . . 18
2.12. Minado con FPGA. Beneficios brutos obtenidos para un periodo de tiempo determinado, expresado en dólares. . . . 18
2.13. Minado con FPGA. Beneficios netos obtenidos para un periodo de tiempo determinado, expresado en dólares. . . . 18
2.14. Minado con tarjetas gráficas ATI/AMD. Beneficios netos obtenidos para un periodo de tiempo determinado, expresado en dólares. . . . 19
2.15. Minado con tarjetas gráficas Nvidia. Beneficios netos obtenidos para un periodo de tiempo determinado, expresado en dólares. . . . 19
2.16. Minado con PC. Beneficios netos obtenidos para un periodo de tiempo determinado, expresado en dólares. . . . 19
2.17. Bienes o servicios y precio al que se comercializan en la darknet. . . . 20

4.1. Comandos descubiertos en el virus. . . . 30
4.2. Parte del EULA de MyFreeProxy. . . . 35

A.1. Tabla resumen con hardware tipo ASIC . . . 43
A.2. Tabla resumen con FPGAs . . . 44
A.3. Tabla resumen de las tarjetas gráficas ATI AMD . . . 55
A.4. Tabla resumen de las tarjetas gráficas Nvidia . . . 59
A.5. Tabla resumen de los dispositivos ARM . . . 60
A.6. Tabla resumen de dispositivos AMD . . . 61
A.7. Tabla resumen de dispositivos Intel . . . 63
A.8. Tabla resumen del resto de dispositivos . . . 64

1

Introducción

Bitcoin, también conocido por sus siglas BTC, es una de las muchas monedas virtuales que han aparecido en los últimos años. Su atractivo principal radica en que la validez de las acciones realizadas con ella se basan en la criptografía fuerte, lo que permite un sistema descentralizado independiente de cualquier organización, incluyendo bancos o gobiernos.

Aunque Bitcoin no pretende ser una moneda anónima, tal y como veremos en el desarrollo de este proyecto, es difícil establecer una relación entre las transferencias y la persona física tras las mismas, siempre y cuando el usuario tenga el suficiente cuidado y no realice ciertas acciones, como cambiar Bitcoins por moneda "analógica" (dólares, euros, etc.).

En cuanto a su funcionamiento, los usuarios de Bitcon forman parte de una red P2P, en la que todas las transacciones realizadas son públicas y quedan registradas en la cadena de bloques, que quedará explicada a lo largo del TFM. Mediante el uso de funciones criptográficas, los usuarios del sistema verifican y validan las transacciones que se van produciendo en el sistema. Esta validación es conocida como *minado*, y cuando un usuario *mina* correctamente un grupo de transacciones, es recompensado por el esfuerzo realizado con una cantidad variable de BTCs, ya que va disminuyendo a medida que se van generando nuevos BTC.

Por lo tanto, se puede deducir que el sistema se autogestiona sin la intervención de terceros de confianza, razón por la cual Bitcoin se ha establecido como una moneda perfecta para realizar pagos en Internet en situaciones que el usuario no quiere ser identificado, como es la compra de sustancias ilegales, armas, servicios de hacking, alquiler de servidores y una larga lista de actividades de dudosa finalidad.

Dado que el valor de 1 BTC es, a principios de Diciembre de 2013, de aproximadamente 790$, han surgido nuevos modelos de negocio en torno a los BTC. Los más destacables son la venta de dispositivos de minado y una nueva generación de malware cuyo fin es utilizar los equipos infectados como nodos de una red distribuida de minado de Bitcoins.

El objetivo del presente documento es analizar la viabilidad de este malware, con el fin de determinar si en un futuro se incrementará la cantidad de variantes del mismo, o si por el contrario, la dificultad del minado de BTC hará que cada vez disminuya el malware cuyo fin sea la extracción de BTC.

1.1 Objetivos

A continuación se lista una relación de los objetvos que se pretenden alcanzar en este TFM:

1. Estudiar el funcionamiento de la red P2P de Bitcoin, haciendo hincapié en la dificultad del minado de los mismos.
2. Analizar el valor de mercado de Bitcoin, y determinar si es factible especular con BTC.
3. Determinar la viabilidad de realizar minería de Bitcoins con ordenadores de uso doméstico.
4. Estudiar los distintos dispositivos que han surgido en los últimos tiempos para realizar minado de Bitcoin, y determinar su viabilidad en el tiempo.
5. Realizar un análisis de muestras de malware cuyo fin es utilizar los equipos infectados para realizar minado de BTC.
6. Establecer el coste aproximado de la realización de dicho malware.
7. Determinar la viabilidad de estos proyectos respecto al tiempo, ya que la dificultad de realizar minado de BTC aumenta en el tiempo.

1.2 Metodología

En este apartado se describe la metodología que se seguirá durante el desarrollo del TFM.

Para estudiar el funcionamiento de la red BTC, el estudiante utilizará la información disponible de manera pública en Internet. Por otra parte, para analizar el valor de mercado de Bitcoin, se estudiarán las distintas casas de cambio de moneda que aceptan Bitcoin, donde se pueden observar las fluctuaciones de BTC en el tiempo.

Tras obtener una lista de los dispositivos de minado más relevantes, se establecerá una relación entre el coste de los mismos, la cantidad y valor de los BTC que pueden extraer, y el coste de la energía necesaria para minarlos.

A continuación, se hará un análisis general de la industria del malware, incluyendo los servicios y precios que se pueden encontrar en la *darknet*, con el fin de conocer la inversión que tiene que hacer un ciberdelincuente para rentabilizar un ataque.

Para la realización del análisis del comportamiento del malware detectado hasta la fecha, además de la información disponible de dicho malware, se emplearán herramientas de análisis como *cuckoo sandbox* e *IDA Pro*, con el fin de determinar que medidas de evasión se emplean, tanto lógicas como humanas. Estas últimas son de vital importancia, ya que el minado de BTC consume ingentes cantidad de recursos, lo que hace que un usuario pueda sospechar de que algo no funciona correctamente y desinfectar el equipo.

Por último, con todos los datos recopilados, el estudiante estará capacitado para determinar si el uso de malware para minar BTC es un negocio rentable, o si por el contrario, cualquier otro método de los mencionados anteriormente permite ganar más dinero en menor tiempo.

1.3 Planificación

Se ha desarrollado un diagrama de Gantt para planificar el trabajo a realizar. En este caso, las tareas se corresponden a los objetivos a conseguir.

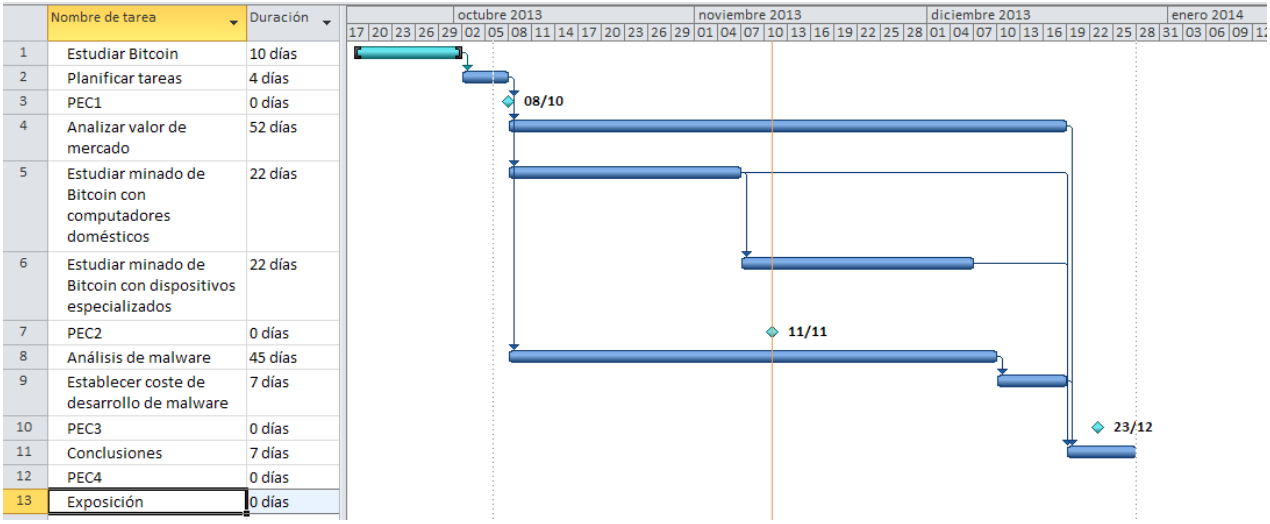

Figura 1.1: Planificación del proyecto

2

Estado del arte

2.1 Conceptos básicos

Bitcoin es una moneda electrónica *Peer-to-Peer* (P2P) descentralizada concebida en 2009 por Satoshi Nakamoto [12, 3]. Bitcoin se basa en la criptografía de clave pública/privada, y cada participante de dicha red tiene una cartera electrónica que contiene un número indeterminado de claves criptográficas.

Las claves públicas se utilizan para emitir o recibir pagos, mientras que las claves privadas se utilizan para autorizar los pagos. Las direcciones Bitcoin son gratuitas e ilimitadas, no contienen ninguna información que permita identificar a su propietario y no requieren de un tercero para su generación.

Un ejemplo del funcionamiento de una transacción es el siguiente:

- Alice transfiere cierta cantidad de BTCs a Bob. Para ello agrega la clave pública de Bob y firma con su clave privada.
- Alice incluye los BTCs en una transacción, y la difunde públicamente a la red Bitcoin.
- Los nodos validan las firmas criptográficas y el valor de la transacción antes de aceptarla y retransmitirla.

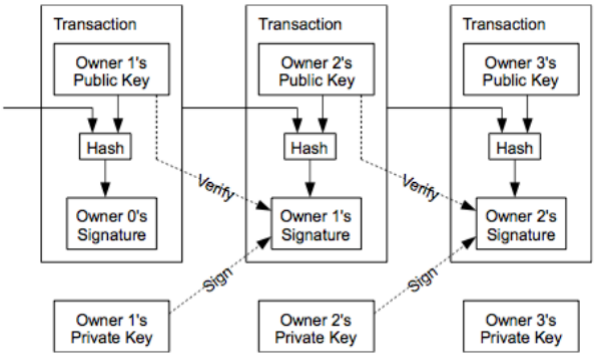

Figura 2.1: Transiciones en la red Bitcoin

Todos los nodos que forman parte de la red Bitcoin mantienen una lista colectiva de todas las transacciones conocidas, a la que se denomina la **cadena de bloques**. Los nodos generadores, también llamados mineros, crean los nuevos bloques, añadiendo en cada uno de ellos el *hash* (en este caso, el resultado de la función criptográfica *SHA-256*[11]) del último bloque de la cadena más larga de la que tienen conocimiento, así como las nuevas transacciones publicadas en la red.

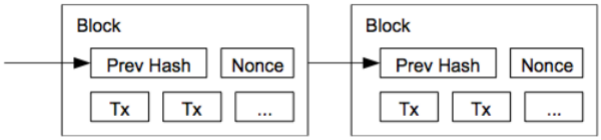

Figura 2.2: Formación de la cadena de bloques en Bitcoin

Cuando un minero encuentra un nuevo bloque, lo transmite al resto de los nodos a los que está conectado. En el caso de que resulte un bloque válido, estos nodos lo agregan a la cadena y lo vuelven a retransmitir. Este proceso se repite indefinidamente hasta que el bloque ha alcanzado todos los nodos de la red. Eventualmente, la cadena de bloques contiene el historial de todas las transacciones que se han realizado en la historia de Bitcoin. De este modo, la red es capaz de rechazar aquellas transacciones que reutilicen Bitcoins ya empleados.

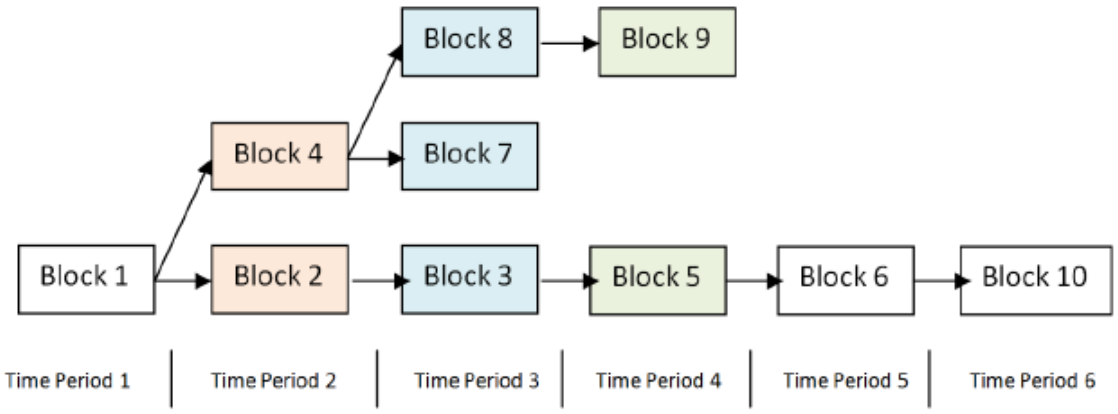

Figura 2.3: Ramas simultáneas en la red Bitcoin. La más larga es la aceptada.

La generación de bloques tiene un concepto similar al de la minería del oro. Los nodos generadores de la red (mineros) compiten para encontrar una solución al problema criptográfico de su bloque-candidato actual. Este problema criptográfico consiste en encontrar un bloque (compuesto por el hash del último bloque de la cadena de bloques, el conjunto de transacciones actuales y un *nonce* o valor aleatorio) cuyo hash tenga una serie de condiciones, como que empiece por un número determinado de ceros.

Para resolver el problema planteado, el minero irá cambiando el valor del nonce hasta dar con la solución por fuerza bruta, ya que no existe ningún algoritmo que permita encontrar la solución de manera sencilla. Este método es no determinista, y garantiza que tras cada intento, las posibilidades de encontrar un bloque válido siguen siendo las mismas[4], ya que la frecuencia de localización de cada bloque sigue una distribución de Poisson. Los nodos que reciben el nuevo bloque solucionado lo validan antes de aceptarlo, agregándolo a la cadena.

La red reajusta la dificultad cada 2016 bloques [5](aproximadamente cada 2 semanas), para que un bloque sea generado cada diez minutos. Cuando un minero encuentra un bloque válido, es recompensado por una cantidad variable de BTCs, nunca superior a 50 BTC, y que disminuye con el paso del tiempo hasta llegar a cero, garantizando que no puedan existir más de 21 millones de BTC. En la actualidad, la recompensa consiste en 25 BTC.

Con el fin de priorizar transacciones, un usuario puede incluir en la transacción una cantidad adicional de Bitcoins, que se almacenarán en la cartera del minero que consiga el bloque válido. Como la recompensa por minar Bitcoins disminuye con el paso del tiempo, en un futuro todos los premios por minar Bitcoins provendrán únicamente de las tarifas de transacción.

Actualmente, los mineros se suelen asociar en *pools de minado*, donde los mineros buscan soluciones a problemas más sencillos que cumplan las condiciones requeridas por la red de Bitcoin[1]. Por ejemplo, si la red de Bitcoin requiere que el hash del bloque comience por 5 ceros, los mineros del *pool* pueden buscar bloques cuyo hash empiece por 2 ceros. Cuando un minero encuentra una solución al problema, percibe una recompensa menor que la ofrecida por la red de Bitcoin, indistintamente de si cumple o no con los requisitos de dicha red. Así pues, llegará un momento que un usuario del pool resuelva el problema de la red Bitcoin, pero el pool lo aceptará como una solución más a su problema particular.

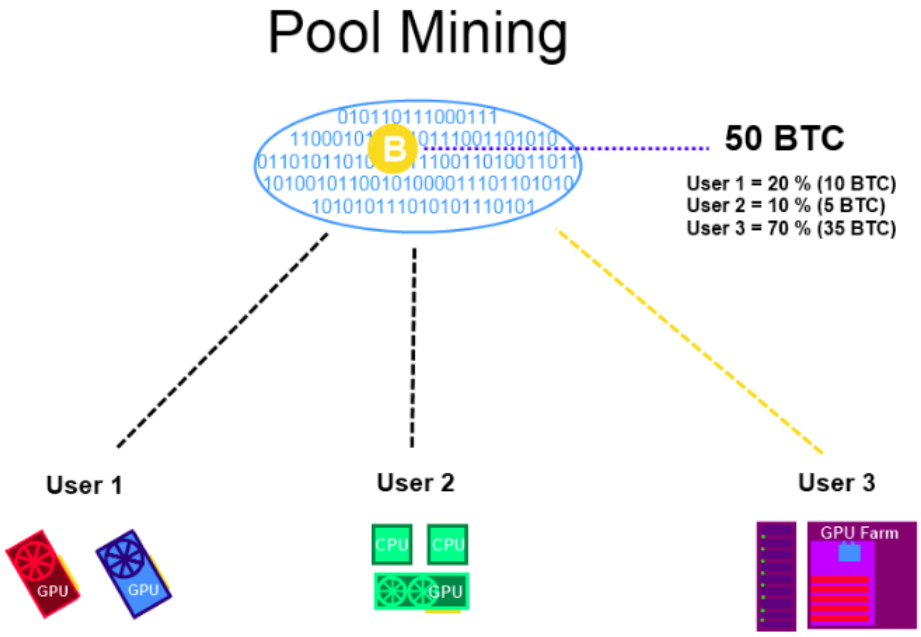

Figura 2.4: Estructura de un *pool* de minado

2.2 Casas de cambio

En Internet existen multitud de sitios web que permiten cambiar Bitcoins por monedas de curso legal. Entre las más conocidas se encuentran BitStamp, btc-e y Mt. Gox. A continuación, se muestra un gráfico con el precio del Bitcoin, en dólares, durante el último año [15].

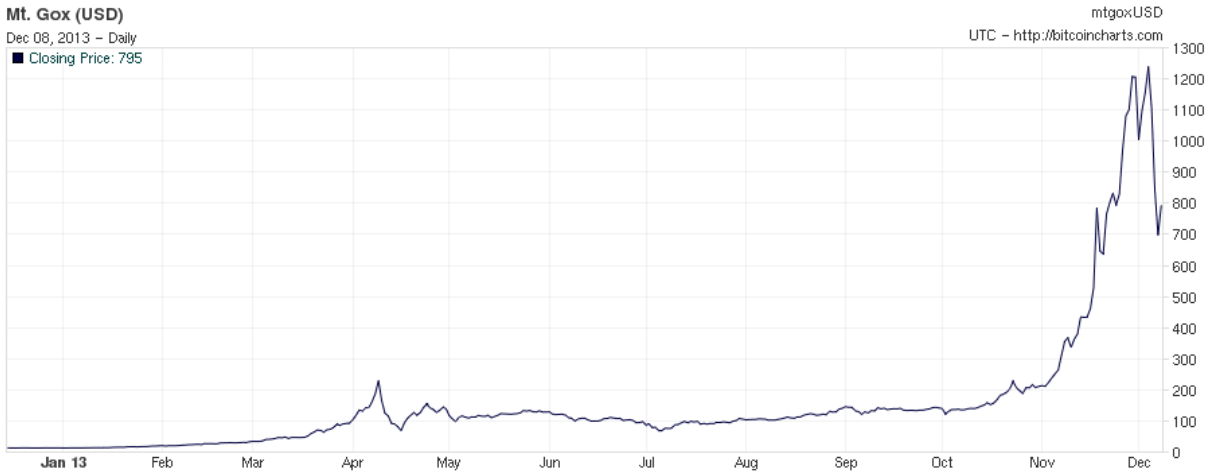

Figura 2.5: Variación del precio del Bitcoin en dólares en MtGox

Figura 2.6: Variación del precio del Bitcoin en dólares en Bitcoin Exchange

Figura 2.7: Variación del precio del Bitcoin en dólares en BitStamp

Como se puede observar en las imágenes anteriores, cualquier persona que hubiese invertido en BTC durante el año pasado, a estas alturas habría ganado en torno al 4937 % de la inversión inicial. Además, un inversor podría predecir cuando va a bajar el valor de Bitcoin monitorizando la actividad de Bitcoin en Internet (cuan activos son los foros, cuantas noticias acerca de Bitcoin aparecen en la red. . .)

Por tanto, invertir en Bitcoin es una oferta tentadora, a la par que legal.

2.2.1. Funcionamiento

Para poder comprar y vender Bitcoins por monedas de curso legal, hay que utilizar los servicios de una casa de cambio. El proceso de utilización es el siguiente:

- Registrarse en la web de cambio. El procedimiento no difiere de otras webs, como Amazon o Facebook.
- Verificación de cuenta. Suele variar dependiendo de webs, pero lo usual es pedir una copia del pasaporte o DNI, una factura o un certificado de empadronamiento.
- Transferencia hacia la casa de cambio. El siguiente paso, es realizar una transferencia hacia la cuenta de la casa de cambio. Dicha cantidad se almacenará como "saldo" disponible del usuario.
- Compra de Bitcoins. Una vez el usuario tiene crédito en la web de cambio, puede comprar Bitcoins. El precio de los mismos varía dependiendo de la oferta/demanda del mismo, estando la cantidad posible de compra limitada al número total de Bitcoins que otro u otros usuarios de la misma casa de cambio esté dispuesto a vender en ese momento. Del mismo modo, un usuario poseedor de Bitcoins, no puede venderlos si nadie está interesado en comprarlos.

Dada la naturaleza on-line the Bitcoin, la mayoría de webs especializadas (incluyendo casas de cambio) ofrecen API [1]

[1] Es el conjunto de funciones y procedimientos que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción

2.2.2. Comparativa

A continuación, se muestra una tabla comparativa de las distintas casas de cambio. El volumen se ha extraído de [17], mientras que las tasas provienen de las webs de las distintas casas.

Nombre	**Volumen (30 días)**	**Comisión mínima**	**Comisión máxima**	**Monedas con las que opera**
Mt. Gox	737,059	0.25 %	0.60 %	Bitcoin
BTC-E	276,578	0.20 %	0.20 %	Bitcoin, Namecoin, Litecoin
bitNZ		0.5 %	0.5 %	Bitcoin
AurumXchange				Bitcoin
Intersango		0	0	Bitcoin
Bitcoin-Central				Bitcoin
ICBIT				Bitcoin
LocalBitcoins				
BTCChina	517,281	0.30 %	0.30 %	Bitcoin
VirWox		50 SLL (León de Sierra Leona) + 2.9 %	50 SLL (León de Sierra Leona) + 2.9 %	
World Bitcoin Exchange		1.1 %	2.0 %	Bitcoin
BitStamp	585,012	0.20 %	0.50 %	Bitcoin
Bitfloor		0.1 %	0.4 %	Bitcoin
Bitcoin24				Bitcoin
Vircurex		0.002BTC	0.002BTC	Bitcoin, Namecoin, Litecoin, PPCoin
LibertyBit		0	0	Bitcoin
Campbx	30,450	0.55 %	2.00 %	Bitcoin
Bitcurex	17,259	0.40 %	0.40 %	Bitcoin
Bitcoin.de	31,386	1.00 %	1.00 %	Bitcoin
Virtex	21,554	0.50 %	1.50 %	Bitcoin
Coinsetter		0	0	Bitcoin
Justcoin				Bitcoin, Litecoin
ITBit	0	0.40 %	0.70 %	Bitcoin

Tabla 2.1: Dispositivos PCI

2.2.3. Anonimicidad y casas de cambio

Antes de utilizar las casas de cambio, hay que tener en cuenta los inconvenientes que presentan. Como se puede deducir, al utilizar los servicios de las casas de cambio se pierde cualquier atisbo de anonimicidad, ya que al almacenar información personal, éstas son capaces de trazar que el usuario que compró X Bitcoins los ha gastado con el usuario Y, ya que las transferencias de Bitcoins son públicas y se pueden consultar en cualquier momento. Además, la existencia de esta información hace que sea posible ser requerida por gobiernos o ser obtenida por cualquier persona o institución por otros métodos, incluyendo las intrusiones en los sistemas de las compañías. Siguiendo este hilo de información, es posible trazar los movimientos realizados por un usuario de Bitcoin.

2.2.4. Ataques a las casas de cambio

Al confiarle el dinero a una casa de cambio, el usuario confía en la seguridad de la misma, característica que no siempre se tiene en consideración. En la siguiente tabla se pueden observar las principales pérdidas de Bitcoins [7].

Nombre	**Época**	**Severidad**
Bitcoin Savings and Trust	2011-2012	263.024BTC
Incautación y cierre de Silk Road	Octubre 2013	17.1955,09292687BTC
Robo de MyBitcoin	Julio 2011	78.739,58205388BTC
Linode Hacks	Marzo 2012	46.653,46630495BTC
Robo de Bitcoinica	Julio 2012	40.000BTC
Hackeo de Bitcoinica	Mayo 2012	18.547,66867623BTC (39.000BTC total)
Robo de Allinvain	Junio 2011	25.000,01000000BTC
Estafa Tony Silk Road	Abril 2012	30.000BTC
Robo de Bitfloor	Septiembre 2012	24.086,17219307BTC
Pérdida Bitomat.pl	Agosto 2011	17.000BTC
Hackeo de Bitcoin7	Octubre 2011	11.000BTC (15.000BTC total)

Tabla 2.2: Perdidas de BTC más significativas hasta el momento en sitios webs.

Cuando una casa de cambio resulta atacada con éxito, como por ejemplo Bitfloor en septiembre de 2012 o Instawallet en el mes de Abril [33], es difícil que el usuario recupere la totalidad de su dinero. Tal y como se puede observar en una casa de cambio que fue cerrada después de ser atacada con éxito, Instawallet (https://www.instawallet.org/), abrió un procedimiento para reclamar el dinero invertido. En él, los usuarios tuvieron 3 meses para formalizar sus reclamaciones, e Instawallet se basó en un sistema de revisión de caso por caso y una política del mejor esfuerzo para aquellos usuarios que tuviesen más de 50 BTC [32].

Por otra parte, durante el pasado mes de Abril, la casa de cambio Mt. Gox [24], que maneja en torno al 70 % de las operaciones de cambios de divisa de Bitcoin, sufrió grandes ataques DDoS [2] que lo desconectó de la red.

[2] Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos

Mientras se produjeron estos ataques, se aprovechó para realizar un phishing del sitio de Mt. Gox. Cuando un usuario abría un enlace, se le instalaba un malware que automáticamente transfería los fondos de las carteras de Bitcoin de las víctimas. [14]

Obviando el ataque Phishing, puede parecer que un ataque de tipo DDoS no permita ganar dinero. Sin embargo, estos ataques se pueden realizar con el fin de provocar que todo el mundo venda sus BTC y conllevando a una bajada de precio del mismo. Aprovechando esta bajada de precios, los atacantes sólo tendrían que esperar a que BTC volviese a subir de precio para venderlos y repetir toda la operacón.

Estos factores, así como la naturaleza especulativa de la compra/venta de Bitcoins hace que su valor varíe con facilidad, aumentando el riesgo de estas operaciones.

2.3 Minado de Bitcoins

Gracias al auge de Bitcoins, han surgido empresas dedicadas a proporcionar dispositivos especialmente diseñados para minar Bitcoins de manera eficiente. De estas empresas, las 3 más conocidas son: ButterflyLabs, Avalon Asics y Mercurybtc.

Figura 2.8: Dispositivos de minado de Butterfly Labs

La siguiente tabla muestra dispositivos PCI que pueden conectarse a un PC de escritorio convencional:

Producto	The Monarch	The Monarch BPU 300 C
Compañía	ButterflyLabs	ButterflyLabs
Precio	4.680$	2.800$
GH/s	600	300
Watios	350	175

Tabla 2.3: Dispositivos PCI

Por otra parte, esta tabla compara dispositivos externos, que van conectados a un PC mediante un cable USB, a excepción del 500 GH/s Bitcoin Miner, que se controla mediante una Nexus 7.

Producto	5 GH/s Bitcoin Miner	50 GH/s Bitcoin Miner	Avalon 4 Module Unit	500 GH/s Bitcoin Miner
Compañía	Butterfly Labs	Butterfly Labs	Avalon Asics	Butterfly Labs
Precio	274 $	2.499 $	8BTC	22.480 $
GH/s	5	60	96	500
Watios	50 [23]	270 [20]	750	2.400[21]

Tabla 2.4: Dispositivos externos

Además, en caso de que las necesidades de su clientes requieran dispositivos de minado personalizados, estas empresas también proporcionan los chips.

Producto	Bobina de 500 Chips A3255	Módulo Avalon 23Gh/s	65 nm ASIC Bitcoin Mining Chip
Compañía	Avalon Asics	Avalon Asics	ButterflyLabs
Precio	30 BTC	1,5 BTC	75$
GH/s	1,4Gh/s por chip (700 Gh/s en total)	23	4
Watios	2,05 W por chip (1025 W en total)	187	12,8

Tabla 2.5: Chips especializados

Por último, está la opción de alquilar la potencia de cálculo en la nube, lo que tiene la ventaja de que el consumo energético y el mantenimiento es costeado por la empresa propietaria del servicio. (Estos servicios se han ofertado durante el año 2013 [8], para el año 2014, los planes han cambiado).

Potencia	1 Gh/s	5 Gh/s	15 Gh/s	30 Gh/s
Precio	48 $	236 $	696 $	1.368 $
Duración del contrato	1 año	1 año	1 año	1 año

Tabla 2.6: Servicios en la nube de mercurybtc.

Como se puede observar, todos los dispositivos aquí mencionados tienen un coste de inversión elevado. Además, su rentabilidad no es clara, puesto que si bien en el momento que son anunciados pueden rentabilizarse en días, estos dispositivos no suelen ser enviados hasta pasados varios meses, por motivos de demanda y de fabricación. Unido a la dificultad creciente del minado de Bitcoins, hace más que posible que en el momento de que un comprador reciba un producto, no sea rentable en su tiempo de vida útil.

2.3.1. Análisis de los dispositivos de minado

En esta sección se estudiarán los beneficios que se pueden obtener minando bitcoins con distintos dispositivos. Para ello, utilizaremos el siguiente algoritmo escrito en Python:

```
from math import pow, log

def profits(difficulty, hashRate, powerConsumption, electricityRate, btcBlock,
    conversionRate, timeFrame, profDeclinerYear):
  hashTime = difficulty * ( pow(2,32) / (hashRate * 1000000.0))
  powerCostPerYear = 365.25 * 24.0 * powerConsumption / 1000.0 *
     electricityRate
  blocksPerYear = (365.25 * 24.0 * 3600.0) / hashTime
  coinsPerYear = btcBlock * blocksPerYear
  revenuePerYear = coinsPerYear * conversionRate
  anteilFrame = timeFrame / 12.0
  factorAverage = 1.0
  if profDeclinerYear != 1:
    factorAverage = (pow(profDeclinerYear, anteilFrame) - 1.0) / log(
       profDeclinerYear) / anteilFrame
  powerCostPerFrame = powerCostPerYear / 12.0 * timeFrame
  revenuePerFrame = revenuePerYear / 12.0 * timeFrame * factorAverage
  return revenuePerFrame - powerCostPerFrame
```

El algoritmo calcula los beneficios en un periodo específico de meses en base a:

- Dificultad de encontrar un nuevo bloque en comparación a lo fácil que puede ser.
- Mhash / segundo.
- Consumo de energía.
- Precio de la electricidad por kWh.
- Bitcoins por bloque.
- Ratio de conversión.
- Periodo de tiempo (meses)
- Descenso de la rentabilidad por año, compensando la variación del precio del Bitcoin y la dificultad del minado.

A continuación se muestran los beneficios que darían los dispositivos vistos en la sección 2.3, junto con algunos dispositivos de uso doméstico. Dada la imposibilidad de realizar un estudio con todos los dispositivos lanzados al mercado, se ha realizado una selección con equipo de gama baja, media y alta. En el anexo A se facilitan los datos necesarios para realizar los cálculos con otros dispositivos existentes.

Los parámetros de entrada elegidos son los siguientes:

- **Dificultad** 707408283,00
- **Mhash / segundo** Indicado por el dispositivo
- **Consumo de energía** Indicado por el dispositivo
- **Precio de la electricidad por kWh** 0,13 €(0,17 $) [29]
- **Bitcoins por bloque** 25,00
- **Ratio de conversión** 790,00 ($/BTC)
- **Periodo de tiempo (meses)** 3, 6 y 12 meses.
- **Descenso de la rentabilidad por año** 0,61.

Los resultados obtenidos son una **estimación**. Dada la volatibilidad del mercado, no se pueden realizar predicciones con exactitud.

Producto	Beneficio bruto (a 3 meses)	Beneficio bruto (a 6 meses)	Beneficio bruto (a 12 meses)
The Monarch	28.814,6920208	54.264,6963468	96.589,6728821
The Monarch BPU 300 C	14.407,3460104	27.132,3481734	48.294,8364411

Tabla 2.7: Dispositivos PCI. Beneficios brutos para un periodo determinado, expresado en dólares.

Producto	Beneficio neto (a 3 meses)	Beneficio neto (a 6 meses)	Beneficio neto (a 12 meses)
The Monarch	24.134,6920208	49.584,6963468	91.909,6728821
The Monarch BPU 300 C	11.607,3460104	24.332,3481734	45.494,8364411

Tabla 2.8: Dispositivos PCI. Beneficios netos para un periodo de tiempo determinado, expresado en dólares.

Producto	Beneficio bruto (a 3 meses)	Beneficio bruto (a 6 meses)	Beneficio bruto (a 12 meses)
5 GH/s Bitcoin Miner	222,581302256	417,12354039	734,749415684
50 GH/s Bitcoin Miner	2.793,91877708	5.251,36878468	9.308,76558821
Avalon 4 Module Unit	4.351,79755332	8.165,24507549	14.420,1349811
500 GH/s Bitcoin Miner	-652,922947744	-1.333,88495961	-2.767,26758432

Tabla 2.9: Dispositivos Externos. Beneficios brutos para un periodo de tiempo determinado, expresado en dólares.

Producto	Beneficio neto (a 3 meses)	Beneficio neto (a 6 meses)	Beneficio neto (a 12 meses)
5 GH/s Bitcoin Miner	-51,4186977437	143,12354039	460,749415684
50 GH/s Bitcoin Miner	294,918777075	2.752,36878468	6.809,76558821
Avalon 4 Module Unit	-1.968,20244668	1.845,24507549	8.100,13498114
500 GH/s Bitcoin Miner	-23.132,9229477	-23.813,8849596	-25.247,2675843

Tabla 2.10: Dispositivos Externos. Beneficios netos obtenidos para un periodo de tiempo determinado, expresado en dólares.

Producto	Beneficio neto (a 12 meses)
1 Gh/s	113,852083137
5 Gh/s	573,260415684
15 Gh/s	1.731,78124705
30 Gh/s	3.487,56249411

Tabla 2.11: Dispositivos en la nube. Beneficios netos obtenidos a 1 año vista, expresado en dólares.

Producto	Beneficio bruto (a 3 meses)	Beneficio bruto (a 6 meses)	Beneficio bruto (a 12 meses)
butterflylabs mini rig	749,999873372	1.358,68286357	2.215,89749505
x6500 fpga miner	12,8887781805	23,5344312312	39,1090492547
icarus	11,1788319715	20,2266950696	32,891567592

Tabla 2.12: Minado con FPGA. Beneficios brutos obtenidos para un periodo de tiempo determinado, expresado en dólares.

Producto	Beneficio neto (a 3 meses)	Beneficio neto (a 6 meses)	Beneficio neto (a 12 meses)
butterflylabs mini rig	-14.545,0001266	-13.936,3171364	-13.079,102505
x6500 fpga miner	-537,111221819	-526,465568769	-510,890950745
icarus	-557,821168029	-548,77330493	-536,108432408

Tabla 2.13: Minado con FPGA. Beneficios netos obtenidos para un periodo de tiempo determinado, expresado en dólares.

Producto	Beneficio neto (a 3 meses)	Beneficio neto (a 6 meses)	Beneficio neto (a 12 meses)
ATI/AMD 7970 x 3	-217,776038575	-447,04809344	-934,890229569
ATI/AMD 7870 xt	-35,0938569311	-72,9075030822	-155,466279679
ATI/AMD 6990 x2	-223,417124815	-456,591843944	-947,808875342
ATI/AMD 6950	-53,6705378851	-109,76365091	-228,123900085

Tabla 2.14: Minado con tarjetas gráficas ATI/AMD. Beneficios netos obtenidos para un periodo de tiempo determinado, expresado en dólares.

Producto	Beneficio neto (a 3 meses)	Beneficio neto (a 6 meses)	Beneficio neto (a 12 meses)
Nvidia tesla s1070	-290,556871018	-581,984074586	-1.167,0565567
Nvidia GTX 680	-31,4664827458	-63,6059030306	-129,599750024
Nvidia GTX 580x2	-76,8168113482	-155,271104041	-316,352871724
Nvidia GTX 295	-101,845608479	-204,368079965	-411,138033565

Tabla 2.15: Minado con tarjetas gráficas Nvidia. Beneficios netos obtenidos para un periodo de tiempo determinado, expresado en dólares.

Producto	Beneficio neto (a 3 meses)	Beneficio neto (a 6 meses)	Beneficio neto (a 12 meses)
4xOpteron 6174	-113,669791798	-227,984482071	-458,257410439
Athlon 64 x2 6400+	-46,4294737497	-92,8752101566	-185,808128959
Phenom II X6 1100T	-45,5080551701	-91,1394822223	-182,716754171
Pentium III	-19,4285566939	-38,8593004348	-77,7263616876
Core 2 Quad Q6600	-38,587615085	-77,2369161111	-154,692727085
Core i5 2400	-35,175636853	-70,3765088636	-140,842565626
Core i7 3930K	-45,2192454239	-90,811971182	-182,949251263

Tabla 2.16: Minado con PC. Beneficios netos obtenidos para un periodo de tiempo determinado, expresado en dólares.

Cómo se puede observar en las tablas anteriores, el minado doméstico de Bitcoins requiere de una inversión en equipo o servicios para que éste empiece a ser rentable. El uso de dispositivos domésticos (PCs, tarjetas gráficas...) no está recomendado, dado que el coste de la energía requerida es mayor que los resultados obtenidos, sin contar el coste de la inversión.

Por otra parte, antes de comprar un dispositivo de minado hay que tener en cuenta el tiempo que se tardará en recibirlo, puesto que para ese momento, el precio y/o la dificultad del minado de Bitcoins habrá variado.

Los cálculos anteriores asumen que la dificultad de los Bitcoin aumentará con el paso del tiempo, tal y como ha venido sucediendo hasta ahora. De acuerdo con esta asunción, minar Bitcoins será menos beneficioso con el paso del tiempo.

2.4 Cibercrimen

En la actualidad, existe un modelo de negocio al margen de la ley conocido como cibercrimen. Estas empresas, tienen una organización y *modus-operandi* similar al de la mafia, y por sorprendente que parezca, se organizan en los mismos departamentos (líderes de la organización, programadores, técnicos expertos, departamento de finanzas...) que una empresa tradicional [30].

A continuación se muestra los bienes o servicios que se ofrecen en la darknet y sus precios[16]:

Bienes o servicios	Rango de precios
Visa y Master Card (EEUU)	4$
American Express (EEUU)	7$
Discover Card (EEUU)	8$
Visa y Master Card (UK, Australia y Canadá)	7-8
American Express (UK, Australia y Canadá)	12-13
Discover Card (Australia y Canadá)	12$
Visa y Master Card (UE y Asia)	15$
Discover y American Express Card (UE y Asia)	18$
Credit Card con pista 1 y 2 (EEUU)	12$
Credit Card con pista 1 y 2 (UK, Australia y Canadá)	19-20
Credit Card con pista 1 y 2 (UE, Asia)	28$
Identidad completa estadounidense	25$
Identidad completa (UK, Australia, Canadá, UE, Asia)	30-40
Tarjeta verificada por VISA(EEUU)	10$
Tarjeta verificada por VISA (UK, Australia, Canadá, UE, Asia)	17-25
Fecha de nacimiento (EEUU)	11$
Fecha de nacimiento (UK, Australia, Canadá, UE, Asia)	15-25
Cuenta bancaria con 70,000$-150,000$	300$ y menos
1000 ordenadores infectados	20$
5000 ordenadores infectados	90$
10000 ordenadores infectados	160$
15000 ordenadores infectados	250$
Troyano de acceso remoto (RAT)	50-250
Complementos para RAT	20-50
Sweet Orange Exploit Kit (alquiler)	450$ semana/1800$ mes
Hacking de un sitio web y robo de datos	100-300
Ataques DDoS (hora)	3-5
Ataques DDoS (día)	90-100
Ataques DDoS (semana)	400-600
Obtención de toda la información de un individuo	$25-$100

Tabla 2.17: Bienes o servicios y precio al que se comercializan en la darknet.

2.4.1. Phishing

En el *Phishing*, el cibercriminal se hace pasar por una tercera persona para conseguir datos sensibles de la víctima. Generalemente, el atacante facilita el enlace a una página de su propiedad que imita a cierta entidad (una red social, un banco...), mediante un correo electrónico, mensajería instantánea o llamadas telefónicas.

En la actualidad, el Phishing ha evolucionado, y se utilizan distintas técnicas para engañar a la víctima con mayor eficiencia y facilidad.

- **Pharming**. El pharming consiste en conseguir, utilizando diversas técnicas, que un dominio DNS ya registrado apunte a una dirección arbitraria propiedad del atacante, donde se estará sirviendo una página similar a la del servicio que se quiera impersonar.
- **Kits de Phishing** A través de Internet, no es difícil comprar un Kit de Phishing. Un Kit de Phishing, no es más que un paquete de webs clonadas, ya preparadas para su instalación en pocos clicks, que permite que la campaña de Phishing se centre sobre múltiples objetivos de manera fácil y sin requerir de grandes dotes informáticas para su uso por parte del delincuente.
- **Herramientas de phishing** Existen herramientas que permiten preparar campañas de Phishing. Probablemente, la más conocida sea *SET* (Social Engineering Toolkit), una herramienta de uso sencillo, con asistentes y que se integra a la perfección con otras herramientas, como *Metasploit*. Cabe resaltar, que SET esta diseñado para realizar ataques sobre el elemento humano, y que el Phishing es sólo uno de los múltiples vectores de ataques que existen.

2.4.2. Troyanos

Los troyanos tienen una larga trayectoria, y son uno de los malware más conocidos por el público no especializado. En los últimos tiempos, los troyanos han evolucionado para sus dueños consigan rentabilidad económica a través de ellos.

Para ello, existen los conocidos troyanos bancarios, como Zeus, Spy Eye, Citadel... Además, el ordenador infectado (conocido como zombie) pasa a formar parte de una red compuesta por otros zombies (conocida como botnet), administrada desde un servidor de C&C (Command and Control). El uso de esta botnet está disponible para su uso mediante alquileres, cuyo precio varía por cantidad de máquinas y tiempo de uso. Generalmente, se utilizan para realizar ataques masivos *DDoS* e incluso para controlar a los dueños legítimos de los ordenadores infectados, permitiendo extraer sus datos personales (incluyendo números de tarjetas y pines).

2.4.3. Ransomware

El Ransomware es un tipo de Malware que "secuestra" el PC de la víctima, bloqueando su uso hasta que la víctima paga una cantidad de dinero al dueño del malware. Existe una variedad de Ransomware que cifra ciertos tipos de ficheros (como documentos de Office, PDFs, vídeos y fotos...) con una clave que solo el dueño del malware conoce. Una vez recibido el pago, el delincuente descifra los ficheros... o no.

Uno de los ransomwares más conocidos hasta la fecha es el conocido "Virus de la Policía".

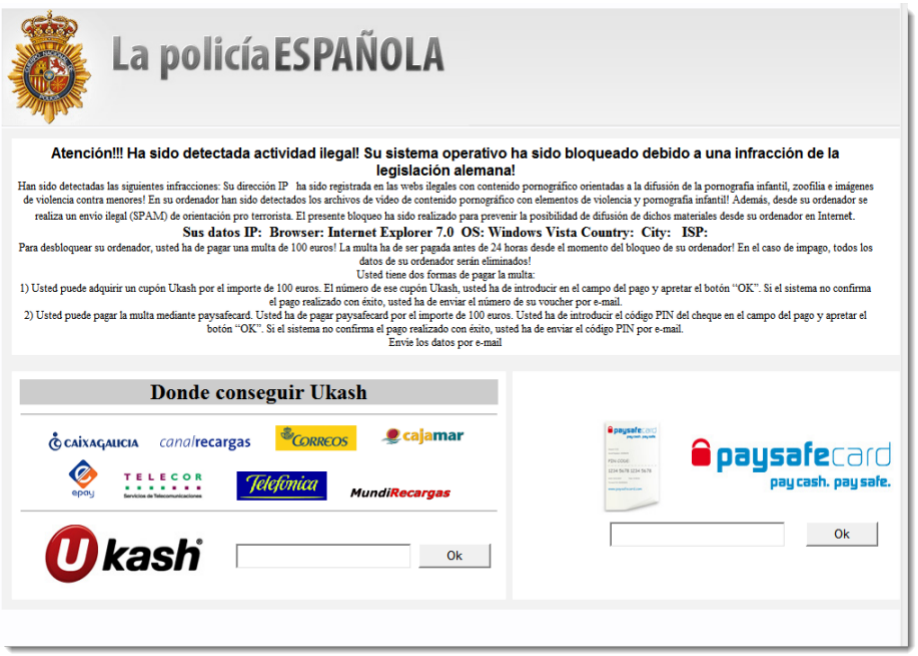

Figura 2.9: Captura de pantalla del "Virus de la Policía"

2.4.4. Exploit Kits

Los *Exploit Kits* son otro de esos packs que se pueden comprar en la darknet, y contienen múltiples *exploits* con los que aprovechar vulnerabilidades de las víctimas y tomar el control de sus máquinas. Los métodos de distribución varían: desde Ingeniería Social (SPAM, mensajería instántanea, etc.) hasta comprometer un sitio seguro y distribuir el malware desde ahí, como por ejemplo lo que sucedió con el sitio de PHP (`http://www.php.net`) recientemente [19].

Una vez el sistema ha sido vulnerado, el sistema forma parte de una botnet y es controlado por los atacantes desde un C&C.

3

Configuración del laboratorio

Para analizar el malware obtenido, se dispone de dos alternativas: la primera, consiste en instalar y configurar un laboratorio con *Cuckoo Sandbox*, mientras que la segunda consiste en utilizar el servicio gratuito mlwr.com (https://malwr.com/). Dado que el objetivo del proyecto es ante todo, aprender y conocer nuevas técnicas de análisis de malware, el estudiante optó por la primera opción.

Cuckoo Sandbox es un software escrito en Python que se puede descargar de http://www.cuckoosandbox.org/download.html o de su repositorio Git git://github.com/cuckoobox/cuckoo.git. Los requisitos del sistema pueden encontrarse en http://docs.cuckoosandbox.org/en/latest/installation/host/requirements/.

El sistema base utilizado es Gentoo Linux, el cual tiene soporte para la mayoría de las dependencias. No obstante, se han utilizado repositorios de terceros para satisfacer las dependencias no soportadas. Además de las dependecias obligatorios, el estudiante ha optado por utilizar el software de virtualización VirtualBox y MySQL para ejecutar el malware y almacenar los resultados. El sistema donde se ha ejecutado el malware es un Windows XP Professional SP3, sin ninguna actualización de seguridad posterior, con el firewall deshabilitado y sin ningún antivirus. Por desgracia, la mayor parte de los virus datan de Abril de 2013, y a día de hoy son fácilmente detectables por cualquier antivirus.

Con el fin de que las muestras analizadas no se propagasen a través de Internet o de la red local, se realizó una primera ejecución del malware sin conexión a Internet, monitorizando las conexiones de salida. A continuación, se procedió a ejecutar el malware en un sistema con conexión a Internet, pero prohibiendo cualquier conexión que no fuese hacia los sistemas de C&C o a distribuidores de nuevo malware. A tal efecto, el sistema utilizado fue un microcomputador Alix con un sistema operativo Voyage GNU/Linux (basado en Debian), y con funciones de routing. El firewall empleado para bloquear la salida a Internet fue iptables.

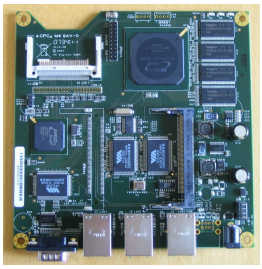

Figura 3.1: Un sistema Alix

Para ejecutar el malware se utilizó el formulario web proporcionado por el mismo Cuckoo Sandbox.

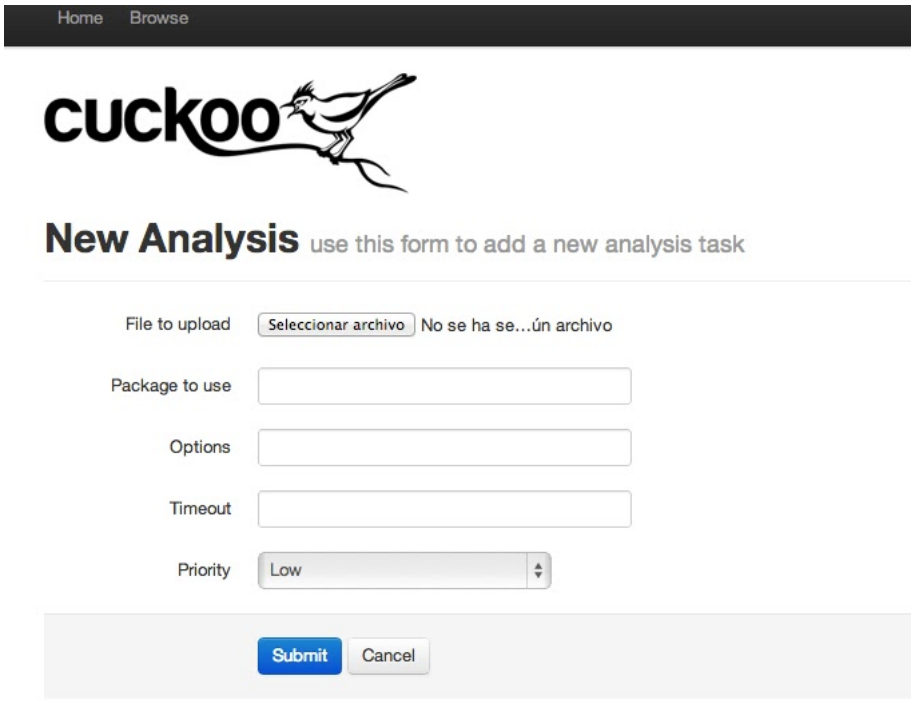

Figura 3.2: Formulario de Cuckoo Sandbox

El único software instalado en el sistema Windows fueron las dependencias del agente de Cuckoo y el propio agente, que permite la comunicación con el servidor maestro.

4

Ataques a Bitcoin

4.1 Malware

En los últimos meses se ha detectado nuevo malware (o variantes de malware conocido) cuyo fin es el de minar y/o robar la cartera de Bitcoins del usuario afectado[13, 18]. De este modo, además de incluir a las máquinas infectadas dentro de botnets, pueden rentabilizarlas desde el primer momento.

4.1.1. Malware distribuido a través de Skype

Durante el pasado mes de Abril, algunos usuarios de Skype recibieron un mensaje que decía "esta es mi foto favorita de ustedes" [26], seguido de un enlace acortado hacia goo.gl o bit.ly, que a su vez redireccionaba a los usuarios hacia una web maliciosa desde donde se descargaba un fichero comprimido en formato zip. Este fichero contenía un malware, y tal y como se puede observar en las estadísticas de ambas páginas, recibió más de 60.000 visitas en un corto periodo:

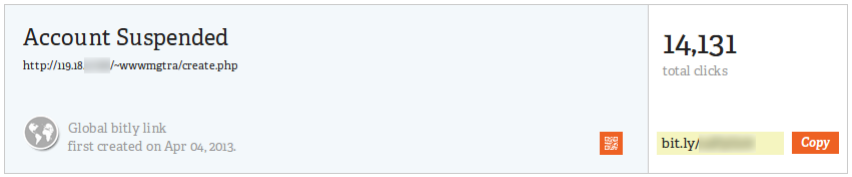

Figura 4.1: Número de visitas recibidas desde bit.ly

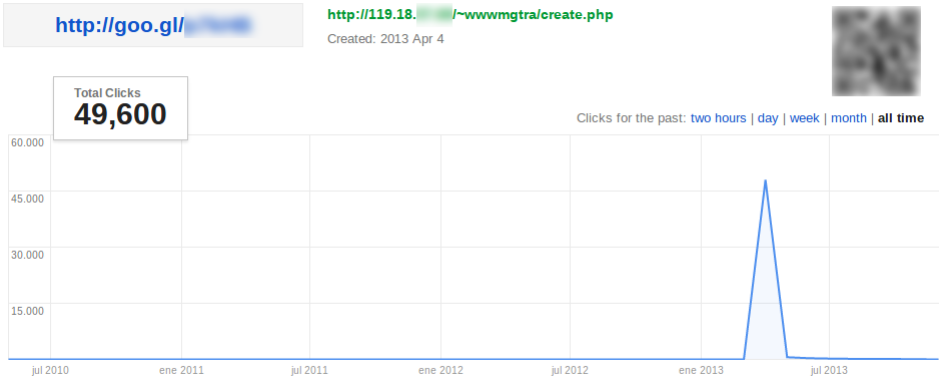

Figura 4.2: Número de visitas recibidas desde goo.gl

La mayoría de estas visitas se produjeron principalmente desde Rusia, Ucrania, Polonia, Alemania, Italia, Brasil, Colombia, EEUU y España.

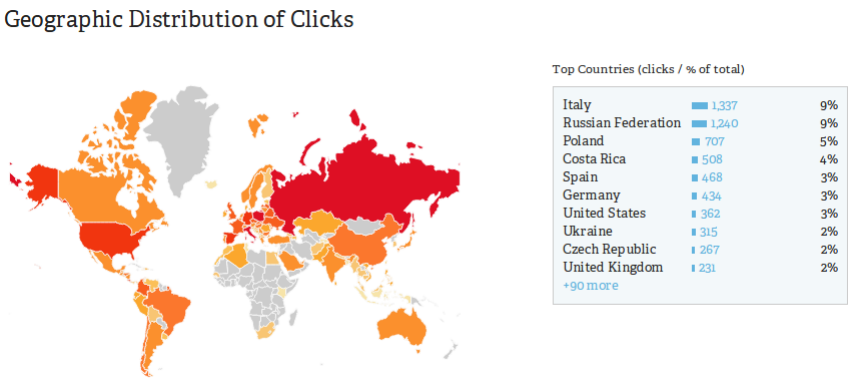

Figura 4.3: Peticiones de bit.ly por país

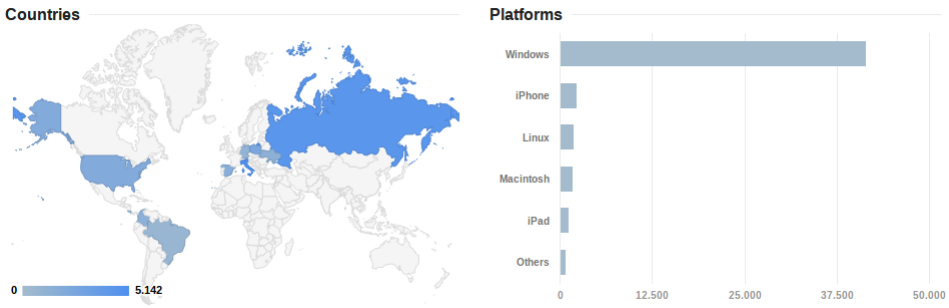

Figura 4.4: Peticiones de goo.gl por país

Aunque la muestra era practicamente indetectable el día que comenzó la distribución, casi todos los antivirus actualizados a día de hoy son capaces de detectarla:

SHA256:	411e93206a7750c8df25730349bf9756ddba52c1bc780eaac4bba2b3872bc037
File name:	xxxxxxo.exe
Detection ratio:	6 / 46

Figura 4.5: Análisis realizado con *Virus Total* el día de su descubrimiento.

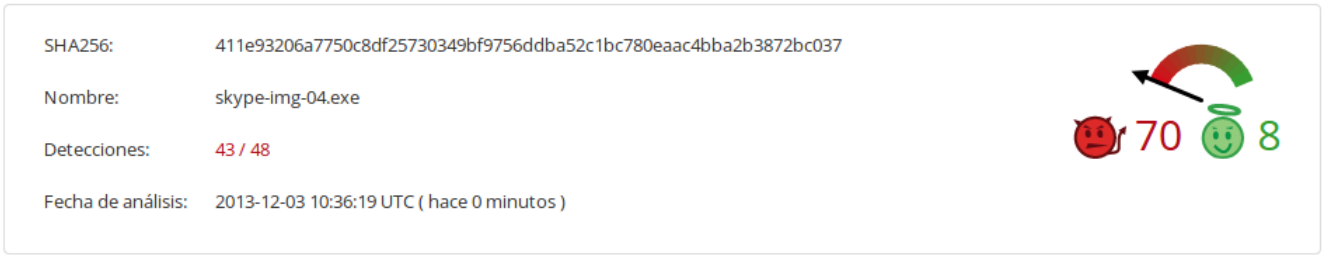

Figura 4.6: Análisis realizado con *Virus Total* el pasado mes de diciembre

Este malware, cuya ofuscación impidió un análisis con IDA Pro, se comunicaba mediante IRC con el servidor de C&C, y tenía funciones de propagación mediante dispositivos USB y de persistencia en el sistema, puesto que modificaba el registro de Windows para que se ejecutase con el arranque del ordenador.

```
004107F4   PUSH DUMP_sky.00413F10                  ASCII "Infected Drive: %s"
004107F9   PUSH DUMP_sky.00413F24                  ASCII "USB"
004109B7   PUSH DUMP_sky.00413F28                  ASCII "%c: "

0040E97E   PUSH DUMP_sky.00413C40                  UNICODE "Software\
   Microsoft\Windows\CurrentVersion\Run"
```

Por desgracia, la botnet, los servidores de minado y demás direcciones de Internet utilizadas por el malware ya no existen, por lo que no es posible seguir el rastro a los dueños del malware. No obstante, la característica que hace a este malware especial es que utiliza el poder de cómputo de los ordenadores infectados para minar Bitcoins y obtener beneficios económicos. En concreto, utiliza “Ufasoft bitcoin-miner”, en su versión 0.28. Si nos fijamos en la siguiente captura veremos que el miner se comunica mediante HTTP, transmitiendo las claves en claro. De los intentos de conexión del malware al servidor de minado, se observan conexiones con autenticación *Basic*. Si descodificamos el base64 de dicha autenticación, podemos observar como se utilizaba la cuenta de correo bigbob0000001@gmail, cuyo password es *password*. Sorprende, que alguien que se toma tantas molestias para distribuir malware, no se preocupe de establecer un canal de comunicaciones seguro, y que tampoco escoja una contraseña robusta. Como se ha mencionado anteriormente, las direcciones utilizadas ya no están on-line, y la cuenta de correo ha sido deshabilitada.

```
POST / HTTP/1.1
Authorization: Basic YmlnYm9iMDAwMDAwMUBnbWFpbC5jb206cGFzc3dvcmQ=
Content-Length: 43
X-Mining-Extensions: hostlist longpoll noncerange rollntime switchto
User-Agent: Ufasoft bitcoin-miner/0.28 (Windows NT XP 5.1.2600 Service Pack 3)
Host: suppp.cantvenlinea.biz:1942
Cache-Control: no-cache

{"method": "getwork", "params": [], "id":0}
```

Figura 4.7: Comunicación del software de minado con el servidor del Pool

Por último, el malware también descargaba nuevas amenazas. En concreto, descargaba una variante del Kelihos y cuando el ordenador se infectaba, formaba a pasar parte de la Kelihos botnet. Esta botnet fue descubierta hacia diciembre de 2010, y por aquel entonces estaba formada por 45.000 equipos. Su principal objetivo, era el envío masivo de correo no deseado (SPAM). En Septiembre de 2011, Microsoft desmanteló la botnet, aunque apareció una nueva versión de la misma en enero de 2012. Esta vez, 11.0000 ordenadores pertenecían a la misma, que fue desmantelada en marzo de 2012. Por último, y coincidiendo con la distribución del malware analizado previamente, se detectó una nueva versión de la botnet, con 70.000 equipos *zombie*[6]. Además del método visto anteriormente, también se distribuye a través de mensajes de Facebook.

Además de enviar SPAM, el Kelihos también analiza el tráfico que se transmite desde el zombie, recolectando usuarios y contraseñas de los protocolos FTP, POP3 y SMTP. También es capaz de robar las credenciales almacenadas en el sistema, además de la cartera de Bitcoin, en el caso de que el usuario legítimo del sistema haga uso de esta moneda.

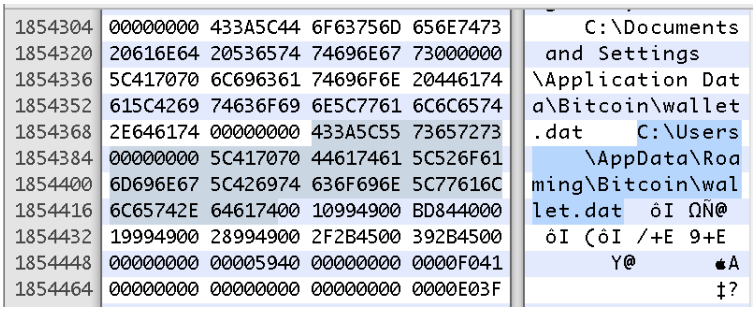

Figura 4.8: Ruta almacenada en una muestra de Kelihos, hacia el fichero *wallet.dat*

4.1.2. Skynet

Usenet es una red de distribución de conocimiento que en los últimos tiempos se ha estado usando para distribuir contenido protegido por los derechos de autor. En este caldo de cultivo, durante el mes de diciembre de 2012 se distribuyó un malware con una baja tasa de detección en VirusTotal (7/42)[22].

El malware estaba compuesto de:

- Un bot de Zeus.
- Un bot controlado mediante el protocolo IRC a través de TOR, con capacidades de DDoS.
- El cliente de minado CGMiner
- Las DLL usadas por CGMiner para hacer uso de GPU.

Nada más ejecutarse, el malware se inyecta en los procesos IEXPLORE o svchost para pasar desapercibido, y además de conectarse a la red TOR, también crea un servicio de acceso a la misma y modifica el registro para ejecutarse tras un reinicio.

El uso de TOR como infraestructura para comunicarse con el C&C tiene ventajas:

- El tráfico va cifrado, evitando la detección por parte de monitores de red.
- La comunicación se realiza con los llamados servicios ocultos de la red TOR, lo que evita que se conozca el origen, localización y naturaleza del C&C, dificultando las posibles acciones para neutralizarlo.
- Al utilizar los servicios ocultos, también se neutraliza la opción de que las autoridades realicen un sinkhole [1] contra el dominio del C&C.
- El dueño de la botnet puede reemplazar el C&C de manera transparente.

A continuación, se muestra una lista de capacidades del Bot:

Acción	**Comando**
Obtener información sobre la máquina infectada	!info !version !hardware !idle
Descargar y ejecutar ficheros	!download
Descargar un binario a memoria e inyectarlo en otro proceso	!download.mem
Visitar una página web	!visit !visit.post
Denegación de servicio mediante flood SYN y UDP	!syn !syn.stop !udp !udp.stop
Flooding Slowloris	!slowloris !slowloris.stop
Flood HTTP	!http.bwrape !http.bwrape.stop
Abrir un proxy SOCKS	!socks
Recuperar las direcciones .onion del servicio oculto abierto en el sistema infectado	!ip

Tabla 4.1: Comandos descubiertos en el virus.

Además de llevar embebido un bot de Zeus, el malware también lleva el cliente de minado libre CGMiner, que permite minar con CPU y GPU. Para pasar desapercibido, el malware monitoriza las pulsaciones de teclas y el ratón. Cuando el sistema lleva 2 minutos sin utilizarse, comienza a minar bitcoins, y para inmediatamente cuando se detecta un uso local del sistema.

Para centralizar y coordinar la minería, los operadores de la botnet emplean un proxy para minado de bitcoins:

Si utilizamos un buscador de malware como *totalhash*, podremos ver como las muestras de malware que tienen relación con bitcoins ascienden, y ya son casi 60 las amenazas detectadas [34].

[1] Un DNS sinkhole, consiste en redireccionar un dominio hacia otra IP, con el fin de que la IP original no sea alcanzable. Se utiliza para parar Botnets, ya que los bots no podrán comunicarse con la dirección que tienen programada para coordinarse.

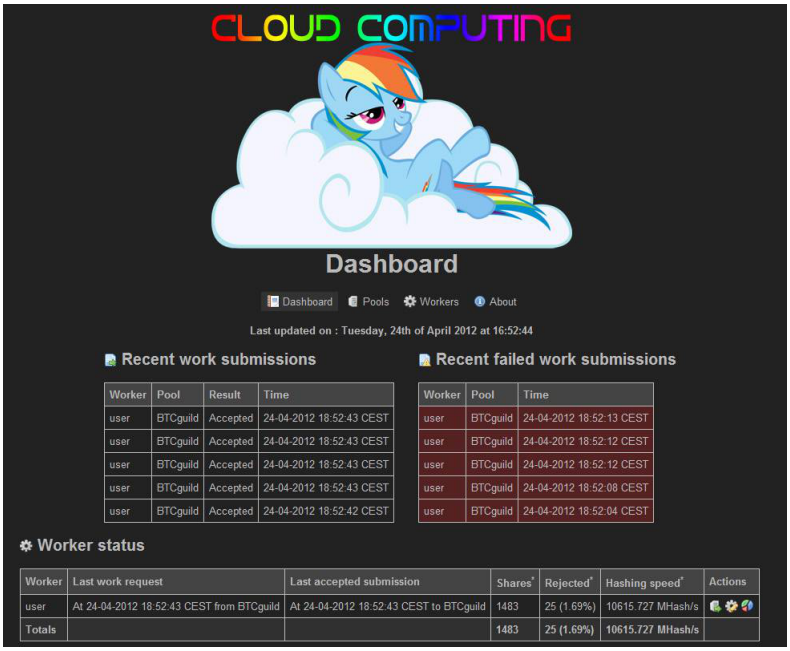

Figura 4.9: Captura del panel de control del proxy de minado de bitcoins

Displaying 1 - 20 of 58 results

SHA1	TIMESTAMP	ORIGIN	SIGNATURE	PACKER
4fabfc7a1a9e5bcdb465ced65460afb0db0f89bf	2013-12-05 17:19:23		Dropper.Agent.AYDF	Pelles C 3.00, 4.00, 4.50 EXE (X86 CRT-LIB)
e2b5bc5b8986ae159700550049fc94370d9dbc90	2013-12-03 22:21:22		TR/BitCoinMiner.N	Microsoft Visual Basic v5.0
e27abdefdf5832be2bb67277c2ad27ef2677e381	2013-11-27 05:23:59		TR/BitCoinMiner.Gen	UPX -> www.upx.sourceforge.net
ff5a5fb94a61f302d578d6174dcfb04ea5ea578a	2013-11-27 03:17:06		TR/BitCoinMiner.Gen	N/A
ea299d6bd24c54139c4705a0fa3ea5ec6d30f752	2013-11-21 20:38:13		object --> 0 <<< TR/BitCoinMiner.Gen	BobSoft Mini Delphi -> BoB / BobSoft
161421f97efbcef3f08d2f0410eb928f43cf4f19	2013-11-08 05:04:21		Win32/DH{Lg9E}	UPX -> www.upx.sourceforge.net
ff28848c5f31f31ee583d479a33ff2e18561645c	2013-11-03 11:53:12		miner.dll <<< TR/BitCoin.L	Microsoft Visual C++ v6.0
3288b9ed9c8d3bafd7ac40befc373485229f0ec2	2013-11-02 06:27:02		TR/BitCoin.B.5	UPX -> www.upx.sourceforge.net
21d6122a0b5d0181596198dd7ee346d8208957dd	2013-11-02 05:36:56		Generic33.BQKR	Microsoft Visual C++ ?.?
0b57bd53e8a0116585cb255ddea603e37ff1d86d	2013-11-01 19:41:45		cpucpu.exe <<< TR/BitCoinMiner.Gen	Microsoft Visual C++ ?.?

Figura 4.10: Resultados de la búsqueda de totalhash

4.2 Phishing

Recurrir a técnicas conocidas como el Phishing también puede ser rentable. Para ello, basta con clonar la apariencia de una web de cambio de Bitcoins y aprovecharse de las vulnerabilidades que presenten los navegadores que accedan a la página maliciosa. En caso de que el navegador sea vulnerable, tras hacerse con el control del sistema, los atacantes pueden obtener el wallet y las credenciales utilizadas en la web legítima. Este tipo de ataque se probó durante el pasado mes de Abril, cuando una web que pretendía hacerse pasar por un chat de MtGOX intentaba aprovechar las últimas vulnerabilidades descubiertas en Java.

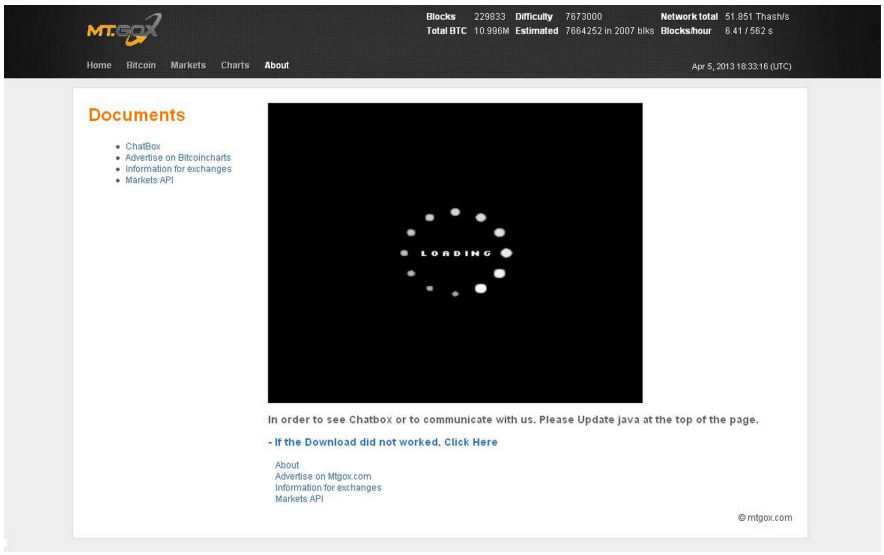

Figura 4.11: Captura de pantalla de una web de phishing centrada en MtGOX.

4.3 Ransomware

Otra técnica que se ha puesto en marcha dado el éxito de Bitcoin es dotar de capacidades de minado al malware de tipo Ransomware. Para ello, una vez se ha bloqueado el acceso al usuario, y mientras se espera que éste pague el rescate de su ordenador, el ransomware se descarga un cliente de minado y utiliza el sistema infectado como minero. Ésta técnica fue encontrada en el ransomware conocido como *Reveton* durante el pasado septiembre de 2013 [25].

Figura 4.12: Captura de pantalla del ransomware Reveton.

4.4 Ataques dirigidos

4.4.1. Ataques de minado

Durante el mes de Junio de 2013, una honeynet propiedad de S2 Grupo detectó ataques automatizados que pretendían aprovechar vulnerabilidades conocidas de PHP. Este tipo de comportamiento es algo usual y no presenta ningún tipo de novedad, pero tras hacerse con el control del sistema, se realizaban las siguientes acciones:

- Descarga y ejecución de un IRC bot escrito en Perl, que se comunicaba con un C&C ubicado en Estados Unidos.
- Descarga del software de minado cgminer.
- Creación de una tarea programada que ejecute el cgminer.
- Ejecución del software de minado, bajo el nombre de apache.

Tras analizar el ataque, se descubrió que se trataba de un burdo copia-pega de varios sitios on-line:

- La distribución se realizaba mediante la explotación de una vulnerabilidad en PHP publicada meses atrás (CVE-2012-1823).
- El IRC Bot se puede obtener fácilmente a través de Internet.
- El cliente utilizado era cgminer, un software de minado opensource.

Mediante la explotación de la vulnerabilidad mencionada, el atacante obtenía una shell remota de PHP, ejecutándose con los permisos con los que se estuviera ejecutando el servidor web. En nuestro caso, el servidor web era un Apache 2 ejecutándose con permisos de root. Obtenido el control del sistema, se descargaba el software de minado mencionado y creaba una tarea programada en el cron.hourly, la cual comprobaba cada hora si el software se estaba ejecutando y en caso contrario, lo ejecutaba. Con estas acciones, se pretendía obtener un rendimiento económico de manera fácil, y no se comprobaba en ningún momento el uso de CPU del sistema. De las acciones vistas, se deduce que de haberse producido en un sistema en producción, el ataque habría sido detectado nada más se disparase el uso de la CPU, puesto que no se realizaba ninguna acción de ocultación, como es el uso de rootkits o la eliminación de los registros del servidor web.

4.4.2. Robo de bitcoins

Atacar con éxito a una casa de cambio de Bitcoins es altamente rentable. Tal y como se ha podido ver en 2.2, los robos pueden suponer el cese de negocio en la plataforma afectada, y los usuarios de la misma probablemente pierdan parte o toda su inversión en Bitcoins.

4.5 Minado desde aplicaciones legítimas

Además de todas las amenazas vistas anteriormente, las aplicaciones legítimas empiezan a minar Bitcoins en detrimento de los usuarios y en beneficios de los autores del software.

4.5.1. Cliente de ESEA

De acuerdo con las noticias aparecidas durante el pasado mes de mayo de 2013 [27], el cliente de la liga de videojuegos ESEA incluyó código para realizar minado de bitcoins cuando el equipo estaba inactivo.

En este caso, los antivirus detectaban la creación de procesos desde el cliente de ESEA, además de la alta actividad de los sistemas cuando estos no estaban realizando, aparentemente, tarea alguna.

No obstante, un usuario publicó un volcado de memoria del cliente de ESEA, donde se apreciaba claramente la salida de un cliente de minado. Se estima que durante las dos semanas que se estubo ejecutando el código, se generó el equivalente a 3.713 dólares. En este caso, el estado de New Jersey condenó a la empresa a pagar una multa de 1 millón de dólares [28].

4.5.2. MyFreeProxy

Durante el mes de diciembre de 2013, se detectó que la barra del navegador *MyFreeProxy* utiliza el ordenador donde se instala para minar Bitcoins. Para evitar disputas legales, durante el proceso de instalación de la barra de herramientas, el usuario acepta un EULA (*End User Licence Agreement*) dónde dice lo siguiente [2]:

COMPUTER CALCULATIONS, SECURITY: as part of downloading a Mutual Public, your computer may do mathematical calculations for our affiliated networks to confirm transactions and increase security. Any rewards or fees collected by WBT or our affiliates are the sole property of WBT and our affiliates.

Tabla 4.2: Parte del EULA de MyFreeProxy.

En dicho EULA, se notifica al usuario que el ordenador podrá realizar operaciones matemáticas para confirmar transacciones, y que cualquier recompensa o ganancia recolectada son propiedad de la empresa desarrolladora de MyFreeProxy.

4.6 Ataques al diseño de Bitcoin

Por último, Ittay Eyal y Emin Gün Sirer[31], del departamento de ciencia de computadores de la universidad de Cornell publicaron un *paper* llamado "Majority is not Enough: Bitcoin Mining is vulnerable", donde se explica un procedimiento para centralizar y controlar la red Bitcoin.

Básicamente, la idea consiste en crear un *pool* lo suficientemente grande (respecto a capacidad de proceso) y que esté controlado por un único elemento llamado *master*. Este pool minaría tanto la cadena de bloques "oficial", como una cadena "clandestina" creada a partir de un bloque determinado, y que iría creciendo de manera paralela y secreta a medida que se resuelven bloques para la misma.

Basados en unas reglas que han definido en el *paper*, llegará un momento en que la cadena del pool egoísta es más larga que la pública, por lo que la publicación de la misma invalidará la cadena "oficial".

En ese instante el proceso del pool egoísta toma valor en la red, invalidando las transferencias del resto de la red.

5

Conclusiones

A lo largo de este documento hemos visto todas las alternativas disponibles para obtener dinero a través de Bitcoin. Entre las opciones legítimas, las más lucrativas son la compra/venta de Bitcoins a través de las casas de cambio y los dispositivos de minado. No obstante, como cualquier otra inversión, tienen sus riesgos: el mercado de Bitcoins es altamente volátil y maleable, mientras que los dispositivos de minado generalmente conllevan una inversión alta para el minero doméstico, además de que las estimaciones pueden resultar papel mojado gracias a los altos tiempos de espera que existen para obtener uno.

El uso de dispositivos domésticos (sistemas x86 comunes, tarjetas gráficas (incluyendo las de última generación), ...) no son recomendables por su alto consumo energético y su pobre potencia de minado frente a dispositivos especializados como son los ASIC o los FPGA. No obstante, desde el punto de vista de un ciberdelincuente, pueden tener utilidad dado que la inversión en equipo o en energía no corre de su cuenta. Solamente por esta razón se explica el incremento de malware con funciones de minado visto en los últimos meses.

Respecto a la pregunta "¿Es rentable el malware de Bitcoins?" Tristemente, la respuesta es sí: la mayoría de malware no se construye ex profeso, sino que que se adopta código de otro malware, o si tiene arquitectura modular, a medida que va pasando el tiempo se activan nuevas funcionalidades y se desactivan aquellas que han quedado obsoletas, abaratando enormemente el coste de creación y mantenimiento. Por otro lado, un ciberdelincuente podría recurrir a otros ciberdelincuentes para alquilar el software o los sistemas infectados para evitar precisamente el coste de creación y mantenimiento del malware.

Además, un cibercriminal no tiene porque centrarse únicamente en la minería de Bitcoins, ya que ésta puede combinarse con otras tácticas: robo completo de la cartera de Bitcoins, secuestro de la información del sistema, robo a través de la banca on-line... El único límite lo establece la imaginación del ciberdelincuente.

Por tanto, es perfectamente posible que en los próximos meses se vea un incremento del malware que intenta aprovechar Bitcoin u otras monedas electrónicas con el fin de conseguir mayor rentabilidad, por lo que los usuarios de este tipo de moneda debería bastionar sus equipos de acuerdo al valor que contienen.

Referencias

[1] 50BTC. 50btc.com. https://50btc.com/, 2013.

[2] Charles Arthur. Bitcoin mining malware could be hidden in app, security researchers warn. http://www.theguardian.com/technology/2013/dec/02/bitcoin-mining-malwarebytes-app-pc.

[3] Múltiples autores. Bitcoin - wikipedia. http://es.wikipedia.org/wiki/Bitcoin.

[4] Múltiples autores. Bloques - bitcoin wiki. https://en.bitcoin.it/wiki/Block.

[5] Múltiples autores. Difficulty - bitcoin. https://en.bitcoin.it/wiki/Difficulty.

[6] Múltiples autores. Kelihos botnet. http://en.wikipedia.org/wiki/Kelihos_botnet.

[7] Múltiples autores. List of bitcoin heists. https://bitcointalk.org/index.php?topic=83794.0.

[8] Múltiples autores. Mercury btc: mining-contracts provider. https://bitcointalk.org/index.php?topic=293127.0.

[9] Múltiples autores. Mining hardware comparison. https://en.bitcoin.it/wiki/Mining_hardware_comparison.

[10] Múltiples autores. Namecoin. http://en.wikipedia.org/wiki/Namecoin.

[11] Múltiples autores. Protocol specification - bitcoin wiki. https://en.bitcoin.it/wiki/Protocol_specification.

[12] Múltiples autores. Página principal - bitcoin wiki. https://es.bitcoin.it/wiki/Página_principal.

[13] Jaime Blasco. How cybercriminals are exploiting bitcoin and other virtual currencies. http://www.alienvault.com/open-threat-exchange/blog/how-cybercriminals-are-exploiting-bitcoin-and-other-virtual-currencies.

[14] Alistair Charlton. Bitcoin traders robbed as mt. gox exchange attacks continue. http://www.ibtimes.co.uk/bitcoin-exchange-ddos-attacks-continue-traders-robbed-456466.

[15] Bitcoin Charts. Bitcoin charts. http://bitcoincharts.com/.

[16] Elizabeth Clarke. The underground hacking economy is alive and well. http://www.secureworks.com/resources/blog/the-underground-hacking-economy-is-alive-and-well/.

[17] coincompare.com. Exchanges. http://coincompare.com/.

[18] CSIRT-CV. El mercado negro del cibercrimen al descubierto. http://www.csirtcv.gva.es/es/noticias/se-disparan-los-robos-de-datos-privados-y-los-ataques-webs-de-bit
html.

[19] David García. Comprometen el sitio oficial de php. http://unaaldia.hispasec.com/2013/10/comprometen-el-sitio-oficial-de-php.html.

[20] David Gilson. Butterfly labs ship first bitforce sc 60 bitcoin miner. http://www.coindesk.com/butterfly-labs-ship-first-bitforce-sc-60-bitcoin-miner/, 2013.

[21] David Gilson. First of butterfly lab's bitforce 500 gh/s mining rigs seen in operation. http://www.coindesk.com/first-of-butterfly-labs-bitforce-500-ghs-mining-rigs-seen-in-operation/, 2013.

[22] Claudio Guarnieri. Skynet, a tor-powered botnet straight from reddit. https://community.rapid7.com/community/infosec/blog/2012/12/06/skynet-a-tor-powered-botnet-straight-from-reddit.

[23] Lee Hutchinson. We've got a butterfly labs bitcoin miner, and it's pretty darn fast. http://arstechnica.com/gadgets/2013/05/weve-got-a-butterfly-labs-bitcoin-miner-and-its-pretty-darn-fast/, 2013.

[24] Eduard Kovacs. Instawallet fue hackeado mientras que mt gox se vio afectado por un masivo ataque ddos. http://news.softpedia.es/Instawallet-fue-hackeado-mientras-que-Mt-Gos-se-vio-afectado-por-un-masivo-at
html.

[25] Adam Kujawa. Ransomware puts your system to work mining bitcoins. http://blog.malwarebytes.org/intelligence/2013/09/ransomware-puts-your-system-to-work-mining-bitcoins/.

[26] Dr. Avalanche Labs. Falso mensaje de skype - bitcoin mining. http://oberheimdmx.blogspot.com.ar/2013/04/falso-mensaje-de-skype-miner.html.

[27] Francisco López. El cliente para liga de videojuegos de esea, mina bitcoins sin consentimiento del usuario. http://unaaldia.hispasec.com/2013/05/el-cliente-para-liga-de-videojuegos-de.html.

[28] Department of Law & Public Safety Office of the attorney general. Acting attorney general announces $1 million settlement resolving consumer fraud, unlawful access claims against online gaming company. http://nj.gov/oag/newsreleases13/pr20131119a.html.

[29] Preciogas.com. Precio kwh españa. http://www.preciogas.com/faq/precio-kwh-espana.

[30] Panda Security. El mercado negro del cibercrimen al descubierto. http://prensa.pandasecurity.com/wp-content/uploads/2011/01/Mercado-Negro-del-Cybercrimen.pdf.

[31] Ittay Eyal & Emin Gün Sirer. Majority is not enough: Bitcoin mining is vulnerable. http://arxiv.org/pdf/1311.0243v1.

[32] Emily Spaven. Instawallet closes claims process and bitcoin-24 encounters problems in poland. http://www.coindesk.com/instawallet-closes-claims-process-and-bitcoin-24-encounters-problems-in-polan

[33] Bianca Stanescu. Fraudsters steal bitcoins in instawallet cyber-attack. http://www.hotforsecurity.com/blog/fraudsters-steal-bitcoins-in-instawallet-cyber-attack-html.

[34] #totalhash. Malware analysis database. http://totalhash.com/search/av:*bitcoin*%20or%20registry:*bitcoin*.

A

Hardware para el minado de Bitcoins

En este anexo, se muestran las características del hardware que se puede utilizar para realizar minado de Bitcoins [9]

A.1 ASIC

En primer lugar, se muestran las ASIC (ApplicationSpecific Integrated Circuit).

Producto	Mhash/s	Mhash/J	Mhash/s/$	Watios	Precio ($)
Avalon ASIC #1	66.300	107	52,34	620	1.299
Avalon ASIC #2	82.000	117	54,70	700	1.499
BitForce SC 5Gh/s	5.000	166	18,24	30	274
BitForce Little Single	30.000		46,22		649
BitForce Single 'SC'	60.000	250	46,18	240	1.299
BitForce Mini Rig 'SC'	1.500.000		50,16		29.899
BitForce SC 25 Gh/s	25.000		24,01		1.249
BitForce SC 50 Gh/s	50.000		20,00		2.499
BitFury's	120.000	705	56	170	2.160
Bitmine,ch Avalon Clone 85GH	85.000		13	650	6.489
Black Arrow Prospero X1	64.000	1777	267	36	239
Black Arrow Prospero X3	1.344.000	1792	336	750	3999
Blue Fury	2.500	1000	17,8	2,5	140
Block Erupter Blade	10.752	129	53	83	170
Block Erupter Emerald	336				
Block Erupter Sapphire	333	130	56	2,55	6
HashFast Baby Jet – First Batch Backorder	400.000	1143	71	350	5.600
HashFast Baby Jet – Second Batch	400.000	1143	145	350	2.760
HashFast Sierra Second Batch	1.200.000	1143	169	1050	7.080
KnCMiner Mercury	100.000		50,04	250	1.995
KnC Saturn	250.000	400	66	300	2.995
KnC Jupiter	500.000	400	80	600	4.995
Monarch BPU 300 C	300.000	1714	107	175	2.800
Monarch BPU 600 C	600.000	1714	128	350	4.680
TerraHash Klondike 16	4.500	140	18	32	250
TerraHash Klondike 64	18.000	140	20	127	900
TerraHash DX Mini (full)	90.000	140	15	640	6.000
TerraHash DX Large (full)	180.000	140	17,14	1.280	10.500

Tabla A.1: Tabla resumen con hardware tipo ASIC

A.2 FPGA

Esta tabla, resume el hardware de tipo FPGA (Field Programmable Gate Array)

Producto	Mhash/s	Mhash/J	Mhash/s/$	Watios	Precio ($)
Avnet Spartan6 LX150T Development Kit	100		0,10		995
Bitcoin Dominator X5000	100	14,7	0,22	6,8	440
BitForce SHA256 Single	832	10,4	1,38	80	599
Butterflylabs Mini Rig	25.200	20,16	1,64	1.250	15.295
Digilent Nexys 2 500K	5		0,03		149
Icarus	380	19,79	0,66	19,2	569
KnCMiner Mars	6.000		2,15		2.795
Lancelot	400			26	350
ModMiner Quad	800	20	0,75	40	1.069
Terasic DE2115	80		0,13		595
X6500 FPGA Miner	400	23,25	0,72	17,2	550
ZTEX USBFPGA Module 1,15b	90		0,27		325
ZTEX USBFPGA Module 1,15x	215		0,52		406
ZTEX USBFPGA Module 1,15y	860		0,65		1.304

Tabla A.2: Tabla resumen con FPGAs

A.3 Tarjetas Gráficas

Por su diseño, las tarjetas gráficas pueden calcular más hashes/segundo que las CPU, ya que tienen un mayor número de núcleos y por tanto, pueden paralelizar en mayor grado todo el trabajo.

A.3.1. ATI AMD

Las tarjetas ATI AMD, tienen más núcleos que las de la competencia, por lo que son más adecuadas para este trabajo.

Modelo	Mhash/s	Mhash/J	Mhash/s/$	Watios	Reloj (Mhz)
3410	0,89	0,074		12	
4350	6,93	0,346	0,16	20	575
4350	7,2				600
4350	8,14		0,19		730
4350	10,7				730
4550	7,23	0,289	0,13	25	600
4550	7,8				
4570M	8,02	0,297		27	
4570M	9,6	0,300		32	
4650	31,33	0,653	0,44	48	650
4670	36,14	0,613	0,34	59	750
4670	40,11	0,679	0,38	59	800
4670	50		0,47	60	800
4730	72,29	0,657		110	
4770	72,29	0,904	0,72	80	750
4830	55,42	0,583		95	575
4830	61,7				700
4830	64,9				700
4830	66,12	0,503		105	700
4850	75,30	0,685		110	625
4850	84,3	0,766		110	725
4850	87,4	0,79		110	785
4850	90,1	0,819		110	800
4850	101	0,918		110	817
4850x2	150,60	0,602		250	625
4860	67,47	0,519		130	700
4870	78	0,520		150	
4870	88			140	
4870	90,36	0,602		150	750
4870	92,84	0,6189333		150	830
4870	96			140	750
4870	104			140	750
4870	104,2				

4870	104,6	0,872		120	830
4870	112			140	750
4870x2	180,6	0,632		286	800
4870x2	180,72	0,632		286	750
4870x2	203				850
4890	97,1	0,511		190	870
4890	102,41	0,539		190	850
4890	108,3	0,57		190	975
4890	121,5			190	1025
5450	11,99	0,631		19	650
5450	13,74				700
5450	14,12				700
5450	15,36				700
5450	18,10				774
5470	17,10				
5550	40,59	1,041		39	550
5550	62,10				700
5570	59,96	1,538		39	650
5570	62	1,59		39	650
5570	64	1,641		39	650
5570	73	1,872		39	700
5570	86,3	2,397		36	775
5570	94				880
5570	102	1,46		75	950
5650	48	1,37		35	
5650	61,2			35	
5670	71,49	1,117		64	775
5670	72	1,64		44	850
5670	85				900
5670	91				890
5670	100				890
5670	103				900
5670	127,8				850
5750	105				
5750	116,24	1,352		86	700
5750	137				710
5750	146,4				775
5750	154,56	1,45		106	830
5750	170				870
5750	173				875
5750	177				910
5750	190				930
5750 VaporX	195			125	975
5750x2 CF	356				870
5770	156,83	1,452		108	850

5770	171,12				
5770	180	1,406		128	950
5770 Hawk	182				875
5770	185				850
5770	205,58				935
5770	214,5	1,95		108	950
5770	214,7	1,95		108	950
5770	216,5				955
5770	218,35				1000
5770	223	2,23		100	1050
5770	227				1030
5770	233	2,23		100	1050
5770	236				1033
5770	240,61	2,3632		100	1080
5770	241			100	1045
5770	244				1050
5770x2	425			225	960
5830M	120				570
5830	244	1,36		179	800
5830	245	1,28		192	880
5830	248	1,29		192	880
5830	256				900
5830	267				875
5830	272	1,52		179	875
5830	275	1,5714		175	900
5830	285		1,58		960
5830	290				930
5830	290				996
5830	295				980
5830	297				970
5830	300				960
5830	300				970
5830	300				970
5830	305				984
5830	307				996
5830	307	2,25	2,55	125	965
5830	308				990
5830	308				990
5830 black	310				990
5830	311				1000
5830	315				970
5830	316				1015
5830	319		1,77		1030
5830	321				1000
5830	323				900

5830	328				1040
5830	331		4,14		1010
5830	333				1040
5830	334				1040
5830	334				1030
5830	342				1045
5830x2 CF	480				800
5830x2	570				950
5830x2	608				990
5830x6	1967	1,62	1,97		1020
5850	240,77	1,595	1,49	151	725
5850	250,26	1,657		151	725
5850	252	1,575		160	765
5850	255,3	1,593		160	765
5850	264	1,748		151	725
5850	280	1,75		160	765
5850	280				725
5850	282,75	3,06		92,25	666
5850	292	1,825		160	765
5850	298	1,8620		160	765
5850	300	1,5460		194	925
5850	304				725
5850	314	1,8362		171	820
5850	328				875
5850	330				850
5850	331				725
5850	335	1,8611		180	890
5850	344	1,8594		185	890
5850	347				876
5850	354				900
5850	355				900
5850	355				900
5850	356				870
5850	359				900
5850	365				920
5850	367,5				900
5850	369,4				930
5850	372	1,68		220	900
5850	375				940
5850	381				940
5850	382	1,8454		207	995
5850	391			180	725
5850	391				1000
5850	392		2,43		990
5850	397				950

5850	400				1000
5850	404				965
5850	408				999
5850	412				1010
5850	414,8				1018
5850	420				1055
5850	431				1040
5850	432,15				1040
5850x2	620				800
5850x2	702				905
5850x2	720				875
5850x3	1.010				850
5850x4	1360	1,94		700	900
5850x6	2.135				900
5870M	152,5				750
5870M	189,2				850
5870	313	1,665		188	900
5870	313,65	1,668	1,65	188	850
5870	340	1,809		188	850
5870	343	1,824		188	900
5870	355	1,888		188	900
5870	360	1,6822		214	970
5870	379	2,015		188	850
5870	397				930
5870	400	1,9047		210	950
5870	408	1,8888		216	980
5870	414	1,9255		215	975
5870	420	2,0000		210	950
5870	421	1,9581		215	975
5870	421,5	2,007		201	950
5870	430				980
5870	432				985
5870	435				990
5870	437		1,90		960
5870	438	1,9819		221	1000
5870	440	2,0000		220	995
5870	445	2,28	2,34	195	1005
5870	453				980
5870	458				1040
5870	460				1050
5870	460				1020
5870	461				1000
5870	481				1050
5870x2 (CF)	864				900
5870x2 (Ares)	620				850

5870x2 (Ares)	826	0,751		1100	950
5870x2 (Ares)	826	1,18		700	935
5870x2 (Ares)	878	0,585		1500	1000
5870x4	1784		1,29		960
5870x6	2568			1200	970
5970	530	1,803	0,53	294	
5970	535,06	1,820		294	725
5970	560	1,905		294	725
5970	565	1,922		294	725
5970	604	2,054		294	725
5970	645	1,875		344	850
5970	739				795
5970	740	2,1511		344	850
5970	755	2,2076		342	848
5970	802	2,31		347	850
5970	820				
5970	822,2				950
5970	833				930
5970	863,4				955
6310M	9,821	0,545		18	500
6450	27,0	1,5		18	625
6450	32,6	1,918		17	725
6450	37,8			17	
6470M	24,1				
6470M	31,0				
6480G	24,1				
6490M	15,21				
6490M	16,289	0,708		23	
6490M	17,18				
6490M	32,1				
6520G	33,8				400
6530D	40,5				444
6550D(A8 Onboard)	66,2				
6550D	67,6				600
6570	68,0	1,133		60	650
6570	82,1	1,368		60	650
6570	86,0	1,95		44	650
6570	112,0				860
6570	114,0				866
6630M	48,80				
6630M	63,00				600
6670	102,20				800
6670	104,00		1,0		820
6670	110,00		1,0		850
6670	111,77	1,69		66	910

6670	120,1				900
6670	124,0			66	940
6750	142			150	700
6750	167,59				870
6750	172,00				860
6750M	41,48				870
6750M	60				
6770	180				850
6770	202				960
6770	217				960
6770	221				1010
6770	235				1010
6770x2	470				1010
6790	220	1,467		150	800
6790	219	1,467		150	960
6850	171,59	1,351	1,07	127	775
6850	196				850
6850	220	1,236		178	1000
6850	234,8				940
6850	236,0				940
6850	244,2				960
6850	245,1			200	940
6850	250	1,612		155	940
6850	256,2			170	980
6850	262,5				965
6850	267,2		1,67		1010
6850	301,4		1,67		
6870	232,47	1,540	1,22	151	900
6870	245				900
6870	264,5				980
6870	271	1,807		150	940
6870	277,47				940
6870	279	1,847		151	900
6870	281,7	1,172			980
6870	293,13				945
6870	294				980
6870	294				985
6870	295	2,02	1,64	146	950
6870	297				1000
6870	300				940
6870	300	1,72		174	1038
6870	300,06	1,830		164	1020
6870	302				940
6870	307	1,72		174	1001
6870	310				1000

6870	310				1035
6870	310				975
6870	312				975
6870	314				1030
6870	316				1030
6870	320			160	950
6870	321				1050
6870	322	1,882		170	1050
6870	329				1075
6870	332		1,74		1050
6870	339,25				1090
6870	375				1000
6870x2	600				945
6870x4	1150		1,2		900
6870x4	1180			145	950
6870x4	1200			150	970
6930	320				960
6930	370				980
6930	372		1,89		1000
6930x2	700			400	940
6950	272		0,90		900
6950	291				920
6950	295				930
6950	295	1,844		160	810
6950	300				940
6950	314				800
6950	325	1,635		200	885
6950	332	1,95	1,2	170	840
6950	333	1,95	1,2	170	840
6950	338	1,84		184	860
6950	340				895
6950	340				800
6950	343	2,14		160	840
6950	344	2,02	1,27	170	840
6950	344,4				800
6950	349	1,745		200	800
6950	351	1,91		184	860
6950	352,8				820
6950	360	1,8		200	970
6950	360				870
6950	365				925
6950	366,4				850
6950	381				850
6950	383				975
6950	388,4				900

6950	389,9				950
6950	400				895
6950	403				939
6950	408,8				925
6950	410,4				950
6950	417	2,085		200	975
6950	418,8				940
6950	425,3				950
6950	428	2,14		200	1000
6950	432	2,16	1,44	200	1000
6950	432,4				1000
6950	440				990
6950	454,4				1050
6950x2 CF	720			400	900
6950x2 CF	731			400	900
6950x3	1081				860
6950x4	1316	1,513		870	840
6970	323	1,468	0,92	220	880
6970	365	2,28		160	880
6970	370				880
6970	372	1,691		220	900
6970	380				
6970	385	1,964		196	900
6970	388				900
6970	403				MAX
6970	406				950
6970	407				955
6970	414				960
6970	420				975
6970	423		1,20		995
6970	431				976
6970	433				975
6970x2	710				900
6970x2	828				940
6970x3	1243			1000+	910
6990	670	1,94	0,89	346	830
6990	704				830
6990	708	2,05		346	830
6990	744				830
6990	746	1,82		410	880
6990	758				880
6990	771	1,8804		410	880
6990	772	1,8380		420	900
6990	790				900
6990	795				

6990	802				915
6990	835		1,11		890
6990	852				955
6990	865		1,11		890
6990x2	1436	1,848		777	880
6990x2	1640	1,416		1200	1010
6990x2	1700	1,416		1200	1010
6990x2	1740	2,11		825	940
6990x3	2094				900
7750	104,15				800
7750	117,15				900
7750	125,5				830
7750	134	2,66	1,21	50	880
7750	136,1				900
7750	140				950
7770	182			83	1020
7770	213				1150
7790	313				1200
7790	325				1300
7850	287	1.91	1.1	150	950
7850	329			150	1100
7850	363				1241
7870	405				1100
7870	406				1100
7870	422				1165
7870	460				1250
7870 XT	485	3,09	1,8726	157	1200
7870xt	520				1200
7950	510				985
7950	512				1000
7950	550				1060
7950	605				1150
7970	555				925
7970	640				1070
7970	650				1100
7970	650				1100
7970	674				1130
7970	685				1150
7970	685				1177
7970	690				1150
7970	695				1160
7970	710				1200
7970	714				1210
7970	825			214	1290
7970x3	1950	2,6	1,72	750	1100

7970x3	2050	2,41	1,22	850	1150
FirePro V3800	69,0				
FirePro V4800	79,7				775
FirePro V8700	84,8				750
FirePro M5800	61,4				650
FirePro M5800	69,3				650
FirePro M5950	96,7				725
FirePro V5800	119				690
FirePro V5800	144				690
FirePro V5800	161				780
FirePro V7750	35,7				
FirePro V7800	254,85				
FirePro M7740 (M97 GL)	63,0				650
FirePro M7820	150,0				700

Tabla A.3: Tabla resumen de las tarjetas gráficas ATI AMD

A.3.2. Nvidia

Modelo	**Mhash/s**	**Mhash/J**	**Watios**	**Reloj (Mhz)**
ION	1,8	0,067	27	
8200 mGPU	1,2			1200
8400 GS	2,3			
8400 GS	1,6	0,013	128	1238
8400M GS	2,0			
8500GT	2,4			918
8600M GT	4,93			
8600M GT	3,8			
8600GT	5,66			1188
8600GT OC	7,3			1602
8800GT	25	0,24	105	1300
8800GT	24,5	0,23	105	1300
8800GT	31,1	0,296	105	1855
8800GT	31,8	0,303	105	1836
8800GT	34,0		105	1998
8800GTS	16,8	0,109	154	
8800 GTS	18,7	0,124	150	1200
8800 GTS	33,5		150	
8800 GTX	27,5			1404
8800m GTX	16,3			
9300GE	1,57			1300
9300GS	1,69			1400

9300/nForce 730i	2,15			1200
9400GT	3,37	0,067	50	1400
9400M (MacBook)	1,90	0,32	6	700
9500M GS	3,2			950
9500GT	6,75	0,135	50	1400
9500GT	7,30	0,135	50	1400
9500GT	7,10	0,135	50	1767
9600GSO	19,88	0,237	84	1375
9600GSO512	11,75	0,131	90	1625
9600GT	15,66	0,165	95	1625
9600GT Zotac	15			1650
9600GT OC	18,8		lt;0,198	
9600M GS	4,0			1075
9800GT	30,36	0,289	105	1800
9800GT EE	19,7	0,263	75	1375
9800GT OC	29,5	0,283	105	1836
9800GTX	32,54	0,232	140	1688
9800GTX+	32,6	0,232	140	1688
9800GTX+	35,39	0,251	141	1836
9800GTX+	36			
9800GTX+	37,23	0,266	140	1890
9800GTX+	40,20	0,287	140	835
9800GX2	57,83	0,294	197	
9800GX2	28	0,142	197	
G210	3,38	0,111	30,5	1402
G210	3,79	0,124	30,5	1402
GT220	10,8	0,084	128	1360
GT230	15,5	0,161	96	650
GT240	19,37	0,281	69	1340
GT240	21,24			
GT240	28,1			
GT240M	9,8	0,426	23	550
GT240 OC	25,6	0,365	70	1765
GTS250	35,39	0,244	145	1836
GTS250	35,2	0,243	145	1836
GTS250 OC	37	0,255	145	2047
GTX260M	22,5			500
GTX260	35,91	0,178	202	1242
GTX260	44	0,242	182	1242
GTX260c216	40,40	0,236	171	1242
GTX260c216	47,4	0,260	182	1348
GTX260c216	50,00			1050
GTX260c216 OC	52,0			1461
GTX260c216 OC	58,9			756
GTX260c216 OC	60,1			1706

GTX275	50,75	0,232	219	1404
GTX275	58			729
GTX280	46,84	0,198	236	1296
GTX280	64,34	0,289	245	1296
GTX285	64,8			1607
GTX285	53,35	0,262	204	1476
GTX295	89,78	0,311	289	1242
GTX295	120,70	0,418	289	1242
GTX295	117,30	0,406	289	1476
GT 320M (MacBook Air)	6,12			1212
320M (Mac mini 2010)	7,0	0,35	20	450
GT 325M	7,5			990
GT 325M	10,5			325
GT 325M	7,99			
GT330	21,65			
GT 330M	7,97			
GT 330M	10,8			650
GT 330M (Sony Vaio Z)	7,8	0,71	11	1045
GT 330M (Samsung R480)	9,1			575
GTS 350M (Toshiba A6653DV)	17,0	1,214	14	1080
GTS 350M (Toshiba A6653DV5)	20,8			1350
GTS 360M	25,0			
GTS 360M (ASUS G60jx)	20,0			
GTS 360M (ASUS G60jx)	27,2			1720
GT430	20,24	0,413	49	1400
GT440	20,4			1645
GT530	17,9	0,358	50	1400
GT520M	8,9			
GT525M	14,6			
GT540M	16,0			
GT550M	17,08			
GT610M (ASUS K45V)	9,371			738
GT650M (rMBP)	17,8			900
GT650M OC	27,4			
GTS450	45,28	0,427	106	1566
GTS450 (Sparkle One)	40,0			
GTS450	45,28	0,427	106	1566
GTX460SE	56,39	0,376	150	1300
GTX460	66,32			814
GTX460	68,31	0,427	160	1350
GTX460 768MB	57,8			
GTX460 768MB (MSI Cyclone 768D5/OC)	75,1			
GTX460 1GB DirectCU	72,3			
GTX460 1GB DirectCU	89,5			
GTX460 1GB (evga FPB)	71,4			870

GTX460 1GB (evga)	83,1	0,519	160	925
GTX460 (2 cards)	102	0,319	320	1350
GTX460 (2 cards) OC	127	0,374	340	1620
GTX460 1GB OC (2x MsiHawksSLI)	158	0,658	240	930
GTX465	64,41	0,322	200	1215
GTX470	81,98	0,381	215	1215
GTX470	94,7			1414
GTX470	103,7			1520
GTX470	111,9	0,520	215	1650
GTX470	115			1616
GTX470x2	121 ea, (130 burst ea,)			1700
GTX480	101,28	0,405	250	1401
GTX480	140,43			1700
GTX480 AMP!Zotac	140,1			1700
GTX550 Ti	45,0			
GTX560 Ti	67,7	0,39	170	1700
GTX560 Ti	74	0,41	170	822
GTX560 Ti	74,8	0,41	180	1700
GTX560 Ti	81	0,45	180	835
GTX560 Ti	85,1			
GTX560 Ti	100	0,5	200	1000
GTX 560M	39,3	0,38	75	775
GTX560 OC	86,7		lt;0,51	
GTX570	105,83	0,483	219	1464
GTX570	140	0,639	219	750
GTX570	157	0,717	219	850
GTX570	165			925
GTX570	160			925
GTX580	156,6	0,642	244	1544
GTX580x2	2x 146	0,598	244	1544
GTX590	193,1			1215
GTX590	2x 121,48			750
GTX670	112,00	1,1	100	1275
GTX680	127,3			1280
GTX680	110,00			1110
GTX680	120,00	1,2	100	1272
Quadro FX 580	5,7	0,14	40	1125
Quadro FX 770M	5,75			500
Quadro FX 770M	6,39			500
Quadro FX 880M	9,6			
Quadro FX 1600M	6	0,12	50	625
Quadro FX 1800	13,6			
Quadro FX 2000M	23	0,397	58	
Quadro FX 2800M	22	0,293	75	600
Quadro FX 3000M	28,6			

Quadro FX 3600M	36	0,514	70	500
Quadro FX 3800	33,3			
Quadro NVS 135M	1,05	0,1	10	800
Quadro NVS 295	1,7	0,07	23	567
Quadro NVS 3100M	3,6	0,257	14	600
Quadro NVS 4200M	10,0			810
Quadro 5000	67,7	0,445	152	513
Tesla C1060	52,5			1296
Tesla K20	134,8			706
Tesla M2050	79,8			1550
Tesla M2050	94,5			1550
Tesla S1070	155,2		800	1440
Tesla S2070	749,23			1150
GTX280x2	102,7			

Tabla A.4: Tabla resumen de las tarjetas gráficas Nvidia

A.4 CPUs/APUs

A.4.1. ARM

Modelo	Mhash/s	Mhash/J	Mhash/s/$	Watios	Reloj (Mhz)
ARM926EJS	0,187				1200
Marvel Feroceon (88FR131)	0,195	0,224	0,01	0,87	1200
ARM1136EJS	0,11				528
ARM1176JZ(F)S	0,119				412
ARM1176JZ(F)S	0,2			3,75	800
CortexA8	0,125	0,36	0,01	0,35	600
CortexA8	0,2	0,57	0,01	0,35	600
CortexA8	0,365				600
CortexA8	0,435				800
CortexA8	0,44				800
Allinner A10(A8)	0,568			2,5	1000
CortexA9	0,57	1,14	0,01	0,5	1000
CortexA9	1,3				1200

Tabla A.5: Tabla resumen de los dispositivos ARM

A.4.2. AMD

Model	Mhash/s	Mhash/J	TDP	CPU Clock	Mhash/s CPU	Mhash/s GPU	GPU	GPU Clock
4x Opteron 6174	115	0,36	320	2,2 GHz	2,4			
2x Opteron 6172	55	0,24	230	2,1 GHz	2,3			
2x Opteron 6128	32,4	0,141	230	2 GHz	32,4			
Athlon XP 2000+	0,62	0,009	70	1,67 GHz	0,62			
Athlon 64 3500+	1,18	0,013	89	2,54 GHz	1,18			
Athlon 64 X2 3800+	1,73	0,03	65	2,00 GHz	1,73			
Athlon 64 X2 4000+	1,9	0,02	65	2,1 GHz	1,9			
Athlon 64 X2 4400+	2,09	0,032	65	2,3GHz	2,09			
Athlon 64 X2 6000+	2,81	0,02	125	3 GHz	2,81			
Athlon 64 X2 6400+	2,9	0,023	125	3,2 GHz				
Athlon II X2 240e	2,71	0,06	45	2,81 GHz	2,71			
Athlon II X2 250	5,6	0,09	65	3,01GHz	5,6			
Athlon II X4 630	10,7	0,11	95	2,8 GHz	10,7		0,4	
Opteron 8220 x16	25			2,8Ghz	1,5			
Phenom II X3 720	3,8	0,04	95	2,8 GHz	3,8			
Phenom X4 9950 BE	9,3	0,07	126	2,6 GHz	2,32			
Phenom II X3 720	7,2	0,08	95	2,8 GHz	7,2			
Phenom II X4 810	5,0		95	2,8 GHz				
Phenom II X4 810	9,5		95	2,8 GHz				

Phenom II X4 810	10,5		95	2,8 GHz				
Phenom II X4 810	11,5		95	2,8 GHz				
Phenom II X4 955	11	0,09	125	3,2 GHz	11			
Phenom II X4 965	12	0,09	140	3,4 GHz	11			
Phenom II X6 1055T	15,84	0,13	125	2,82 GHz	15,84			
Phenom II X6 1055T	23,6		95	3,50 GHz	23,6			
Phenom II X6 1075T	21,3		125					
Phenom II X6 1090T	18		141	3,50 GHz	3			
Phenom II X6 1100T	22	0,176	125	3,82 GHz	22			
Sempron 3000+	0,8		62	1,6 GHz	0,8			
Turion X2 RM70	1,9		65	2,1 GHz	1,9			
Zacate E350	11	0,615	18	1,6 Ghz	1,231	9,831	HD6310M	492 Mhz
Zacate E350	12			1,648	1,252	10,87	HD6310M	492 Mhz
Ontario C50	6,2	0,68	9	1,0 Ghz	1,200	6,2	HD6250M	277 Mhz
A43400	23,2		75	2,4 Ghz		23,2	6350	
A83850	60		100			60	HD6550D	
A83870K	95		100	3,3 Ghz		95	HD6550D	900MHz
A105800K	105		100	3,8 Ghz		105	HD7660D	800MHz

Tabla A.6: Tabla resumen de dispositivos AMD

A.4.3. Intel

Modelo	Mhash/s	Mhash/J	Mash/s/$	Watios	Reloj (Ghz)
Pentium III (Coppermine)	0,39	0,008		TDP 2x 26,1	1
Pentium III mobile	1	0,3	0,014		21
Pentium M 1,6ghz	0,4				1,6
Pentium M 1,6ghz	0,62				1,6
Pentium M 1,6ghz	0,71				1,6
Pentium M 1,73ghz	0,5				1,73
Old Xeon 512k (Dual)	2,0				3,0
Pentium 4 2,0A	0,85				2,0
Pentium 4 630	1,29				3,0
Pentium DualCore E2180	1,75				2,0
Pentium DualCore E2180	4,1				2,0
Pentium DualCore E2180	4,5				2,0
Pentium DualCore E5400	2,27	0,03		65	2,7
Celeron E330	2,2	0,03		65	2,5
Celeron E3400	5,9				2,6
Core 2 Quad Q6600	11,0		0,02	105	2,40
Core 2 Quad Q8200	10,9		0,06		2,33
Core 2 Quad Q9400	11	0,046	0,06	95	2,66

Core 2 Quad Q9650	18,67		0,05	95	4,00
Core i3 530	8,31	0,10	0,06	80	3,66
Core i3 M350	1,48	0,04		35	2,27
Core i32100	8,28				3,1
Core i5 M450	1,8	0,05		35	1,2
Core i5650	5,1	0,04		0,02	
Core i5750	14		0,06		3,2
Core i5	4	6,5			
Core i52400	4,5	0,05	0,02	95	3,1
Core i52400	14	0,15	0,07	95	3,1
Core i52400S	16,6			65	2,5
Core i5 2500K	20,6		0,10		4,2
Core i5 2600K	17,3			75	3,4
Core i7 2600K	18,6			95 max,	3,4
Core i7 2600	23,9				3,4
Core i7 620M	1,888				2,66
Core i7 620M	6,5				3,33
Core i7 720QM	7,9				45
Core i7 820	13,8				2,8
Core i7 920	19,2	0,10		195	4,0 (x21)
Core i7 950	5,88	0,039		150	3,83 (x23)
Core i7 950	18,9	0,126		150	3,83 (x23)
Core i7 980x	19,2	0,15		130	4,4 (x33)
Core i7 980x	8,7				3,9 (x27)
Core i7 990x	33,3				4,5 (x32)
Core i7 2635QM	2,93				2,00
Core i7 620M	6,3	0,18		35	2,66
Core i7 2600k	6,7				4,00
Core i7 3770k	5,2				4,4
Core i7 3930k	66,6				4,625 (125 x 37)
Core 2 Duo U7600	1,1				1,2
Core 2 Duo E5200	6,2	0,086		72	2,76
Core 2 Duo E6550	2,45				2,33
Core 2 Duo E6850	6,75	0,10		65	3,0
Core 2 Duo E7300	7,76	0,11		70	3,33
Core 2 Duo E7300	2,52	0,04		65	2,66
Core 2 Duo E8200	2,3	0,035		65	2,66
Core 2 Duo E8400	6,9	0,106		65	3,0
Core 2 Duo E8500	3,6				3,16
Core 2 Duo E8500	7,2				3,16
Core 2 Duo P8700	5,9				2,53
Core 2 Duo T5450	2,5	0,07		35	1,63
Core 2 Duo T5500	4,3				1,66
Core 2 Duo T6400	4,2	0,12		35	2,00
Core 2 Duo T7250	4,5	0,13		35	2,00

Core 2 Duo T7450	3,7	0,10		35	2,13
Core 2 Duo T9400	4,2				2,53
Core 2 Extreme X9000	2,37				2,8
Core 2 Extreme X9000	6,2				2,8
Core 2 Extreme X9000	7,2				3,2
Xeon 2,8	0,8				2,8
Xeon 3060	2,03	0,03		65	2,
Xeon Prestonia 2,4 (dual)	2,16	0,017		130	2,4
Xeon X5355 (dual)	10,13	0,16		120	2,6
Xeon E31230 V2 (quad)	19,7				
Xeon X5355 (dual)	22,76	0,09		120	2,6
Xeon X5365 (dual)	26,00				
Xeon X5650	28,6				
Xeon x5680 (dual)	48				
Xeon x5690 (dual)	52				
Xeon E52690 (dual)	66				
Xeon E5335	9,35	0,12		80	2,00
Xeon E5410	9,8				80
Xeon E5440	7,3				80
Xeon E5506	9,6				80
Xeon E5520	6,5	0,08		80	2,27
Xeon E5530	7,14	0,09		80	2,4
Xeon E5620	11,2				80
Xeon E5630 (dual)	8	0,1		80	2,53
Xeon E6520 (dual)	24,7				2,53
Xeon E7220	6,3				80
Xeon E7320 (dual)	1,5				2,8
Xeon E7450 (quad)	60				2,40
Xeon E7520 (dual)	18			95	1,87
Xeon 3680	18			130	3,33
Atom Z520	1,20			2	1,7
Atom N230	0,375			4	1,6
Atom N230	0,245			4	1,6
Atom N230	0,97			4	1,6
Atom N270	1,19	0,24		5	1,6
Atom N450	1,60	0,31		6,5	2,06
Atom N550	1,97				1,5
Atom 330	1,80			8	1,6
Atom D510	1,00				1,6
Atom D510	2,3	0,07		30	1,6

Tabla A.7: Tabla resumen de dispositivos Intel

A.4.4. Otros

Modelo	Mhash/s	Mhash/J	Mash/s/$	Watios	Reloj
Cell	21	0,35	0,07	60	3,2 GHz
Cell	26,6				
Cell	21	0,7	0,07	35	3,2 GHz
MIPS	0,026				
VIA Eden	1,3	0,17		8	1600 MHz
PowerPC 7447A	0,53				1420 MHz
PowerPC 7450 (G4e)	1,29				1670 MHz
PowerPC 750 (G3)	0,140				600 MHz
IBM POER4+ 2/way	0,58				1450 MHz
IBM Power7 (PowerPC)	7,6				3,5 Ghz
Google App Engine	0,144			0	
Open Shift	0,059			0	

Tabla A.8: Tabla resumen del resto de dispositivos

B

Otras monedas

B.1 Litecoin

Litecoin es una moneda virtual muy similar a Bitcoin. Existen 3 diferencias principales con Bitcoin:

- El procesamiento de un bloque de transferencias se realiza cada 2,5 minutos en lugar de cada 10, tal y como venía sucediendo en Bitcoin.
- El número máximo de Litecoins emitidos será de cerca de 84 millones, en lugar de los 21 millones de Bitcoin.
- Litecoin está diseñado para que se pueda minar eficientemente con GPUs, dificultando las implementaciones hardware mediante FPGA o ASIC.

Como se ha podido ver en el apartado 2.2, está moneda comienza a estar soportada por las distintas casas de cambio, y su capacidad de ser minada por usuarios domésticos sin hardware específico hace de ella una moneda especialmente atractiva.

B.2 Namecoin

Namecoin es una criptomoneda basada en Bitcoin, cuyo uso principal es hacer de servidor DNS descentralizado fuera del control de ICANN. En el blockchain, además de los datos incluídos en Bitcoin, también se añaden los registros de dominio. De este modo, para traducir un nombre de dominio a una IP, basta con consultar la cadena de bloques.

Namecoin puede tener otros usos [10]:

- Sistema de autenticación.
- Sello temporal.

- Tracker de torrents.
- Web de confianza.
- Sistema de mensajería.
- Sistema de identidad
- Voto electrónico
- Sistema de alias
- Espacio de nombres personal.
- Sistema público de verificación de integridad de archivos

Glosario

Application Programming Interface (API) Es el conjunto de funciones y procedimientos que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción.. 12

Distributed Denial Of Service (DDOS) Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.. 14

Sinkhole Un DNS sinkhole, consiste en redireccionar un dominio hacia otra IP, con el fin de que la IP original no sea alcanzable. Se utiliza para parar Botnets, ya que los bots no podrán comunicarse con la dirección que tienen programada para coordinarse. 31