

“Necesidades del Estado Colombiano y las entidades públicas en el marco de la Auditoría Forense”

Teniente Coronel FREDY BAUTISTA GARCIA
CENTRO CIBERNÉTICO POLICIAL



@caivirtual
@fredy_secure
www.ccp.gov.co

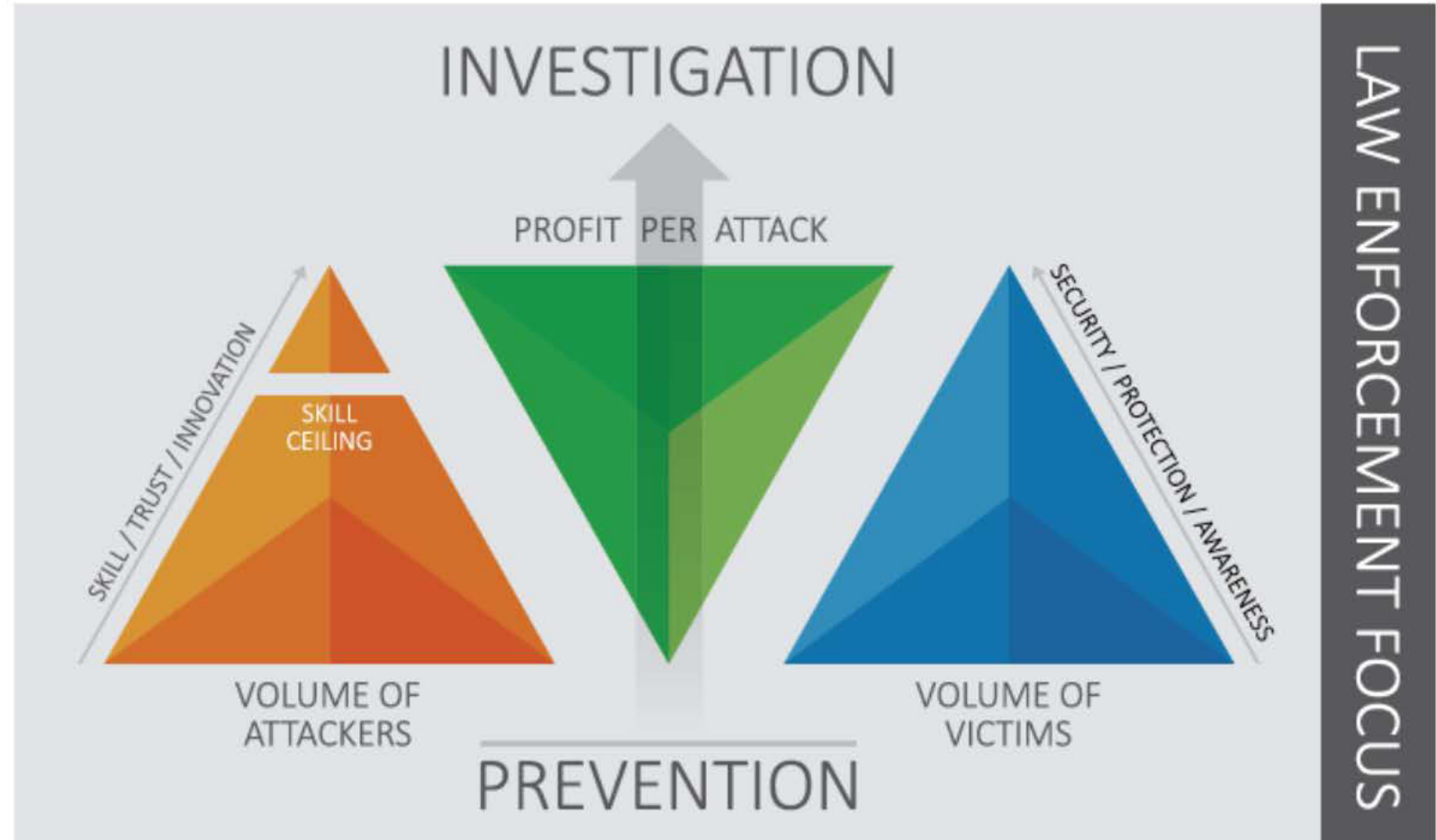
Bogotá DC , Octubre de 2016

Agenda

- Tendencias globales del Cibercrimen
- Crimen Organizado 2.0
- Modelo Crime as Service
- B.E.C. Bussines Email Compromise

1. Tricotomía del Cibercrimen

Visión del cibercrimen



Tendencias Globales del Cibercrimen

- Secuestro de Información
 - Cifrado complejo del dispositivo o de carpetas
 - Cobros Extorsivos BITCOINS y otras criptomonedas
 - Afecta indiscriminadamente empresas y ciudadanos
 - Variante Cryptolocker – sector de arranque
 - Ransomware para móviles
-

Tendencias Globales del Cibercrimen

```
_Locky_recover_instructions.txt.372390.DROPPED x
1      !!! IMPORTANT INFORMATION !!!!
2
3      All of your files are encrypted with RSA-2048 and AES-128 ciphers.
4      More information about the RSA and AES can be found here:
5          http://en.wikipedia.org/wiki/RSA_(cryptosystem)
6          http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
7
8      Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
9      To receive your private key follow one of the links:
10         1. http://twbers4hmi6dx65f.tor2web.org/32C0D883E1644D0A
11         2. http://twbers4hmi6dx65f.onion.to/32C0D883E1644D0A
12         3. http://twbers4hmi6dx65f.onion.cab/32C0D883E1644D0A
13
14     If all of this addresses are not available, follow these steps:
15         1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
16         2. After a successful installation, run the browser and wait for initialization.
17         3. Type in the address bar: twbers4hmi6dx65f.onion/32C0D883E1644D0A
18         4. Follow the instructions on the site.
19
20     !!! Your personal identification ID: 32C0D883E1644D0A !!!          !!! IMPORTANT INFORMATION !!!!
21
22     All of your files are encrypted with RSA-2048 and AES-128 ciphers.
23     More information about the RSA and AES can be found here:
24         http://en.wikipedia.org/wiki/RSA_(cryptosystem)
25         http://en.wikipedia.org/wiki/Advanced_Encryption_Standard
26
27     Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
28     To receive your private key follow one of the links:
29         1. http://twbers4hmi6dx65f.tor2web.org/32C0D883E1644D0A
30         2. http://twbers4hmi6dx65f.onion.to/32C0D883E1644D0A
31         3. http://twbers4hmi6dx65f.onion.cab/32C0D883E1644D0A
32
33     If all of this addresses are not available, follow these steps:
34         1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
35         2. After a successful installation, run the browser and wait for initialization.
36         3. Type in the address bar: twbers4hmi6dx65f.onion/32C0D883E1644D0A
37         4. Follow the instructions on the site.
38
```

Tendencias Globales del Cibercrimen



Attention!

All your main files were encrypted!

ID:

Personal documents , photos and videos were encrypted . Files such as: jpeg , doc , docx , avi , excel , and others will be unreadable.

Encryption was made using a unique public key RSA-2048 generated for this computer.

To decrypt files you need to have a private key.

A unique copy of the private key is located on the special secret server! This key will allow to decrypt Your files!

Remember the main reasons that may cause deleting your private key FOREVER:

- You have only 72 hour to get your private key. Do not waste your time. After 72 hour period Your key will be deleted

- Any attempts to remove this virus/encryption will be unsuccessful. And this is the reason to delete your key too.

- Do not send any emails with threats and rudeness to us. Example of Email format is "Hello! I want to decrypt my files. My ID number is I have attached a file for the free decryption. Waiting for my next instruction"

Please contact us by email, along with an identification number, which is shown in the picture and is specified in the file "HELP_DECRYPT.txt."

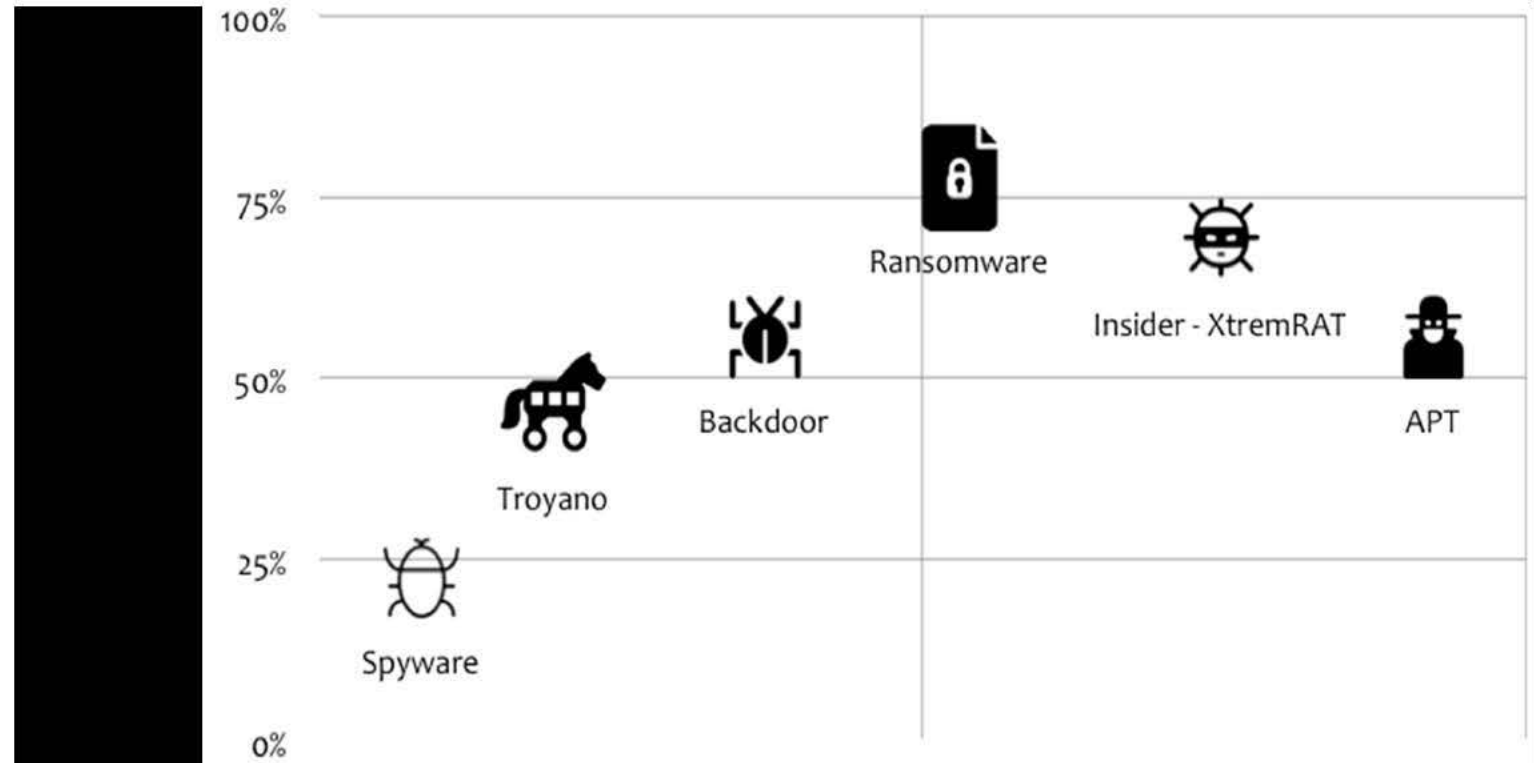
We can remove encryption from a single file for free. Just send it us and then You will receive a decrypted file. It will be your guaranty!

Contact Information :

uniquekey@dr.com

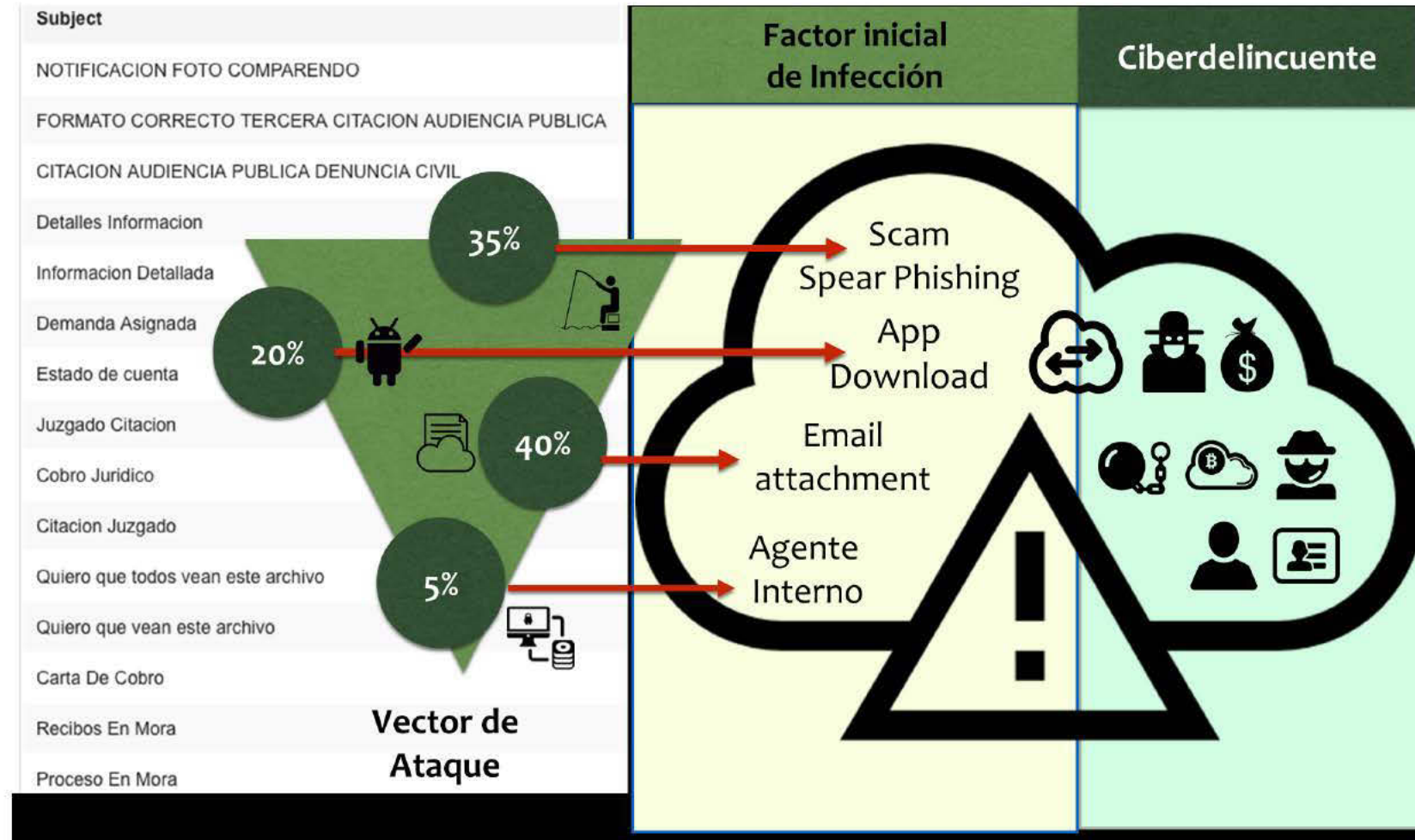
2. Ataques sofisticados de Malware

Tendencias Globales del Cibercrimen



2. Ataques sofisticados de Malware

Tendencias Globales del Cibercrimen



2. Ataques sofisticados de Malware

Tendencias Globales del Cibercrimen

Centro Cibernético @CaiVirtual

¿FotoMalware? Respetemos las normas de tránsito 🚦, pero mucho cuidado si recibe este tipo de correos, es #Malware

Enviado: martes, 5 de julio de 2016 1:54
Para: [Clara](#)
Asunto: Aviso De Fotorrecomparación



#Malware

URL que redirecciona al sitio web fraudulento

BOGOTÁ COLOMBIA
Julio 05 del 2016

Señor conductor se le notifica por el presente correo que ha sido sancionado con una foto multa por sobrepasar un semáforo en rojo lo invitamos a respetar las normas de tránsito y a utilizar la inteligencia vial.

Se le envía a descargar fotos hora y dirección de su fotormulta en el siguiente vínculo

Malware site
<https://securityhome.box.com/shared/static/1xe4yapyjgg4pkkyufmhjk3zs8my0>

Lo invitamos a cancelar su infracción dentro de 5 días hábiles y reciba un 50 % de descuento

RETWEETS 34 ME GUSTA 10

9:40 - 7 jul. 2016

Centro Cibernético @CaiVirtual

¡ALERTA! ➡ correo electrónico que suplanta a @Superservicios podría hurtar toda su información. Evite dar CLIC

Superservicios
Superintendencia de Servicios Públicos Domiciliarios

BOGOTÁ 30 de junio del 2016

Señor(a)

Estimado usuario:

Reciba por parte de la superintendencia de servicios públicos un cordial saludo realizado una consulta personalizada en nuestros bases de datos encontramos que usted presenta varias anomalías en el servicio de energía, por lo tanto le comunicamos se acompaña hasta las instalaciones de la superintendencia de servicios públicos para evaluar el fin de o necesidad entre otros servicios.

El personal técnico de nuestra empresa estuvo realizando las diferentes inspecciones y suministraron 2 tipos de finides que de no aclararse tener un costo de hasta 7 salarios mínimos mensuales vigentes.

Dicha notificación es presentada via internet debido a que en la inspección realizada por el personal técnico no se encontraban personas en el área susceptible.

A continuación adjuntamos las fotos tomadas por el personal que realiza la inspección desde encontramos los diferentes finides: E0201, E0202, E0203, E0204

Atentamente: **WILCIBARRA-GR**
Alfredo Moreno Vargas **FIDERRER-VI-GR**
Gonzalo Jimenez **TRUJAN-GUERRERO-E020019**
Superintendencia de servicios públicos D.C. **HTTP/1.1 200 OK**
WILCIBARRA-GR

#Malware

RETWEETS 39 ME GUSTA 21

12:31 - 7 jul. 2016

Superservicios, Policía de Colombia y DJJIN

2. Ataques sofisticados de Malware

Tendencias Globales del Cibercrimen



¡ALERTA! falso correo de una FOTOMULTA es utilizado para hurtar toda su información. Evite dar CLIC #Malware

The image shows a screenshot of a fraudulent email. On the left, there is a header with a logo and the text '16 DE JUNIO DEL 2016'. Below it, the subject is 'ACTA DE INFRACCIÓN DE TRANSITO' and the body contains details of a traffic violation, including 'SEÑOR CONDUCTOR' and a fine amount of '725.250'. On the right, there is a sidebar with a list of names and IDs, such as 'Oygd BRVY' and 'Togp GeneraD 002068'. At the bottom, there is a green arrow pointing to a button that says 'Descargue sus archivos aquí', with the text 'Resultado del análisis.' above it. A large green arrow points from the button to the right. At the bottom of the screenshot, there is a black box with the text '#Malware'.

RETWEETS 202 ME GUSTA 71

7:14 - 21 jun. 2016

Policia de Colombia y a DIJIN

202 71



Centro Cibernético @CaiVirtual · 22 sept.

¿Quién visitó su perfil de #Facebook? Es solo un truco para propagar software malicioso y obtener información ¡La curiosidad mató al gato! 🐱

The image shows a screenshot of a Facebook profile page. The profile picture is a cartoon cat wearing a hat. The cover photo is a dark blue banner with the text 'Find your profile viewers está en Facebook.' Below the banner, there is a section titled 'Find your profile viewers' with a sub-header 'Comunidad'. The main content of the page is a large advertisement for the 'Find your profile viewers' app, which claims to show who has visited the user's profile. The ad includes a search bar, a list of 'PERSONAS' (10,646), and a 'DESCARGAR' button. At the bottom of the page, there are icons for back, share, and like, with the number '24' next to the share icon and '11' next to the like icon.

Tendencias Globales del Cibercrimen



Tendencias Globales del Cibercrimen



messages(0) | orders(0) | account(\$0.00) | settings | log out

search | (0)

Shop by category:

- Drugs(1462)
- Benzos(153)
- Cannabis(527)
- Dissociatives(26)
- Ecstasy(86)
- Opioids(116)
- Other(148)
- Psychedelics(173)
- Stimulants(137)
- Apparel(4)
- Art(26)
- Books(118)
- Computer equipment(1)
- Digital goods(63)
- Drug paraphernalia(26)
- Electronics(10)
- Food(1)
- Forgeries(17)
- Home & Garden(1)
- Lab Supplies(4)
- Medical(7)
- Money(85)
- Services(34)
- Weaponry(25)
- XXX(43)



10 Neville's Haze Seeds by Black...
\$17.45



SecureVM Basic Fully Custom Config...
\$31.55



10 Early Riser Seeds by Sagarmatha
\$8.88



Tylenol #3 Codeine 500/30 x 20...
\$11.09



2Gram - Mdma Crystals - Special...
\$16.58



Rivotril/Klonopin 2 mg Roche Clonazepam...
\$42.68



Beretta US M9 w/fac. laser NIB...
\$175.97



13 C 13 Haze Seeds by DNA Genetics
\$11.63



AUSSIE SATIVA 7g
\$15.72

News:

- **State of the Road Address**
- Silk Road has a new **URL**
- Announcing the new **wiki**
- New shipping and display **features**

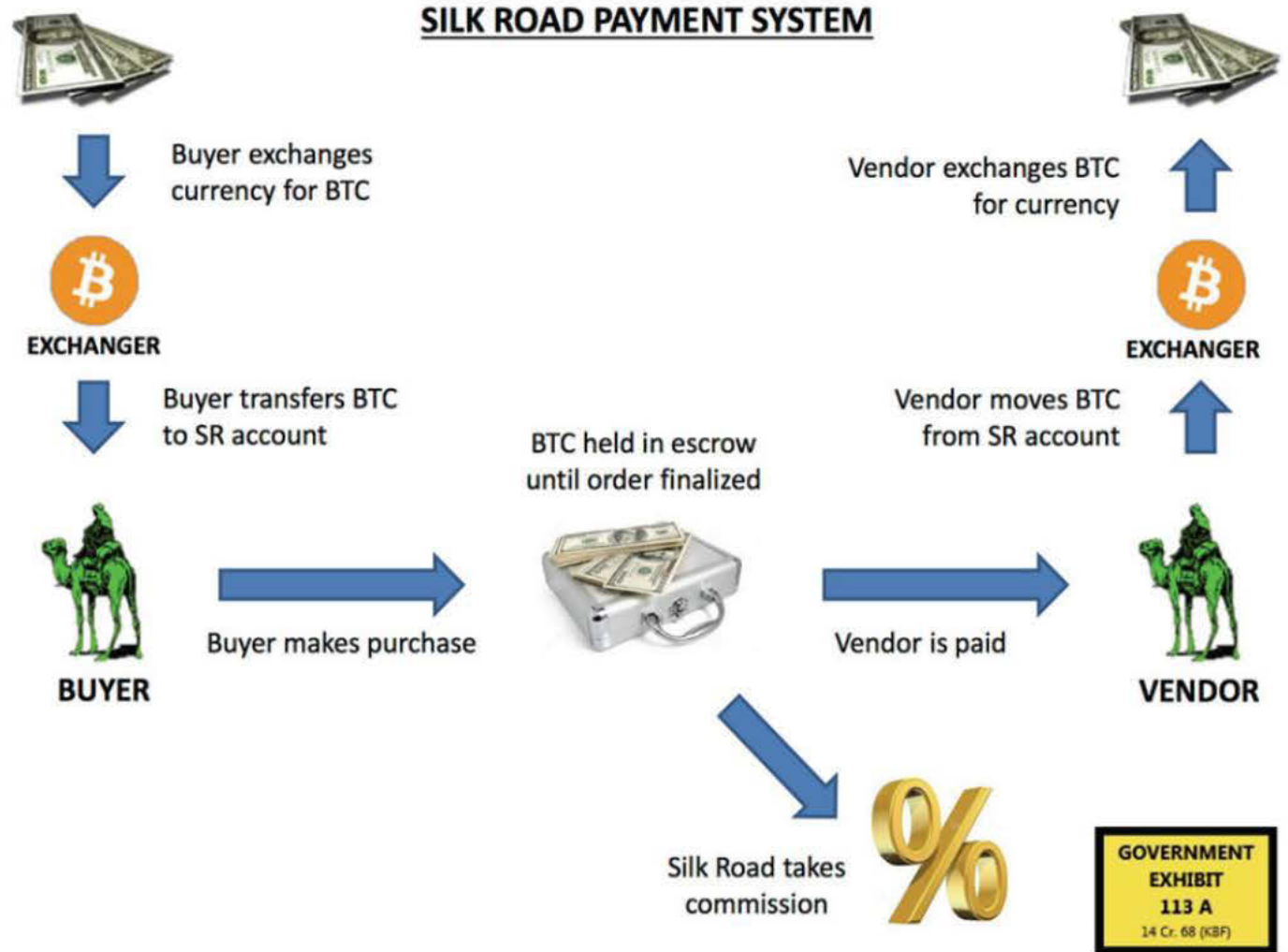
3. Mercados Ilegales

Agora, Pandora, SilkRoad

Tendencias Globales del Cibercrimen

The screenshot displays a dark web marketplace interface. At the top, it shows the exchange rate '1 BTC = 255 USD' and navigation tabs for 'Listings', 'Messages', 'Profile', 'Orders', 'Account', 'Vendor Profiles', and 'FAQ'. Below the navigation, there are filters for 'regular offers' and 'auctions', and a search bar. The main content area is titled 'path: drugs->stimulan' and shows a list of items. The first item is '1g COCAINE HAU' with a price of 'eurc' and a thumbnail image of white powder. The second item is '500mg COCAINE HAU' with a price of 'eurc' and a thumbnail image of a woman. The third item is '0.5g COCAIN' with a price of 'eurc' and a thumbnail image of a woman. Each item listing includes a file name, size, and a download link. The interface is cluttered with various elements, including a sidebar with categories like 'digitalgoods', 'drugs', 'electronics', and 'realgoods'.

Tendencias Globales del Cibercrimen



4. Internet Profunda

Tendencias Globales del Cibercrimen



4. Internet Profunda

Tendencias Globales del Cibercrimen

- No existe consenso en la regulación
- Anonimato
- Oferta ilegal de bienes y servicios
- Transacciones fraudulentas
- TOR y otros programas de navegación profunda
- Generalmente asociado a transacciones fraudulentas

DarkNet

1. Estructuras Criminales del Cibercrimen

Crimen Organizado 2.0



1. Estructuras Criminales del Cibercrimen

Condiciones opcionales

Crimen Organizado 2.0

- Objetivos de perseguir beneficio y/o poder
 - Participantes con función específica
 - Utilizan alguna forma de disciplina y control interno
 - Implican blanqueo de dinero
 - Operan en el ámbito internacional
 - Estructuras similares a las comerciales o de negocios
-

1. B.E.C. Business Email Compromise

B.E.C. Business Email Compromise



1. B.E.C. Business Email Compromise

B.E.C. Business Email Compromise

- Utilice correos corporativos para el uso de los funcionarios
 - Proteja la información de su compañía en redes sociales
 - Sospeche de peticiones de cambios de cuentas para pagar en último momento
 - Separe sus dispositivos corporativos del Internet de las Cosas
 - Establecer un dominio web de la empresa protegido de accesos particulares
 - Utilizar firmas digitales a nivel transaccional
-

1. B.E.C. Business Email Compromise

U.S. Department of Justice
Federal Bureau of Investigation
Office of Private Sector



BUSINESS EMAIL COMPROMISE

Business Email Compromise (BEC) is a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments.

POTENTIAL TARGETS AND METHODS

- Businesses and personnel using open source email
- Individuals responsible for handling wire transfers within a specific business
- Spoof emails that very closely mimic a legitimate email request (e.g. "Code to admin expenses" or "Urgent wire transfer")
- Fraudulent email requests for a wire transfer are well-worded, specific to the business being victimized

IT & FINANCE SECURITY

- Establish more than one communication channel to verify significant transactions
- Use digital signature on both sides of transactions
- Immediately delete unsolicited email (spam) from unknown parties
- Forward emails and include the correct email address to ensure the intended recipient receives the email
- Remain vigilant of sudden changes in business practices

PROTECTING YOUR ORGANIZATION

- Avoid free web-based email if possible
- Establish a company website domain and use it to establish company email accounts
- Be careful what is posted to social media and company websites
- Be suspicious of requests for secrecy or pressure to take action quickly
- Separate your computer devices from Internet of Things (IoT) devices
- Disable the Universal Plug and Play protocol (UPnP) on your router

Internet Crime Complaint Center

- If you believe your business is the recipient of a compromised email or a victim of a BEC scam, file with the Internet Crime Complaint Center (IC3) at www.IC3.gov. Be descriptive and identify your complaint as "Business Email Compromise" or "BEC."

CONTACT US: For questions or assistance, locate and contact your local FBI field office at www.fbi.gov

“Necesidades del Estado Colombiano y las entidades públicas en el marco de la Auditoría Forense”

Teniente Coronel FREDY BAUTISTA GARCIA
CENTRO CIBERNÉTICO POLICIAL



@caivirtual

@fredy_secure

www.ccp.gov.co

Bogotá DC Oct. de 2016
