Universidad Externado de Colombia | FACULTAD DE CONTADURÍA PÚBLICA

"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

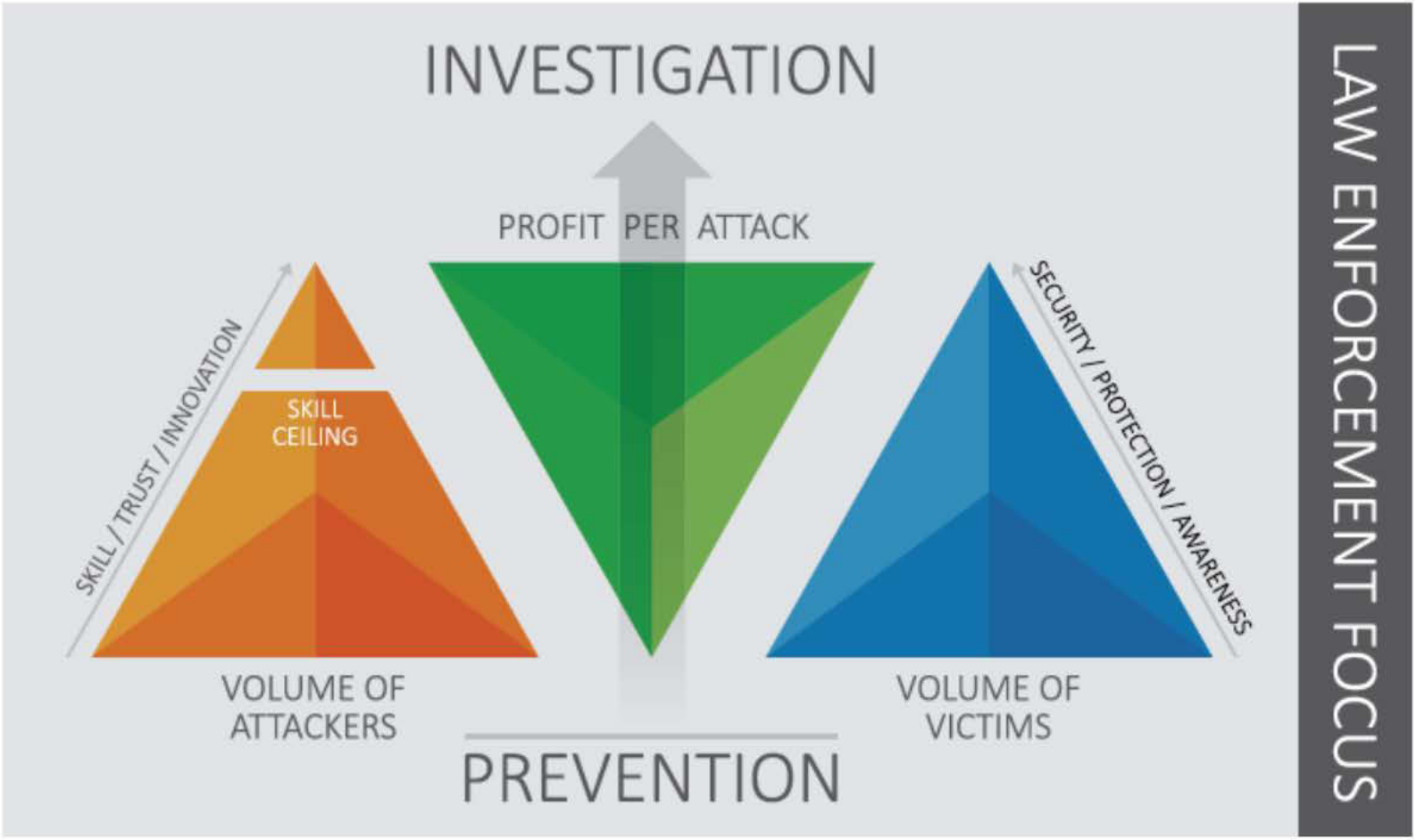
Bogotá DC , Octubre de 2016

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



1. Ransomware

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

1. Ransomware

Tendencias Globales del Cibercrimen

_Locky_recover_instructions.txt.372390.DROPPED

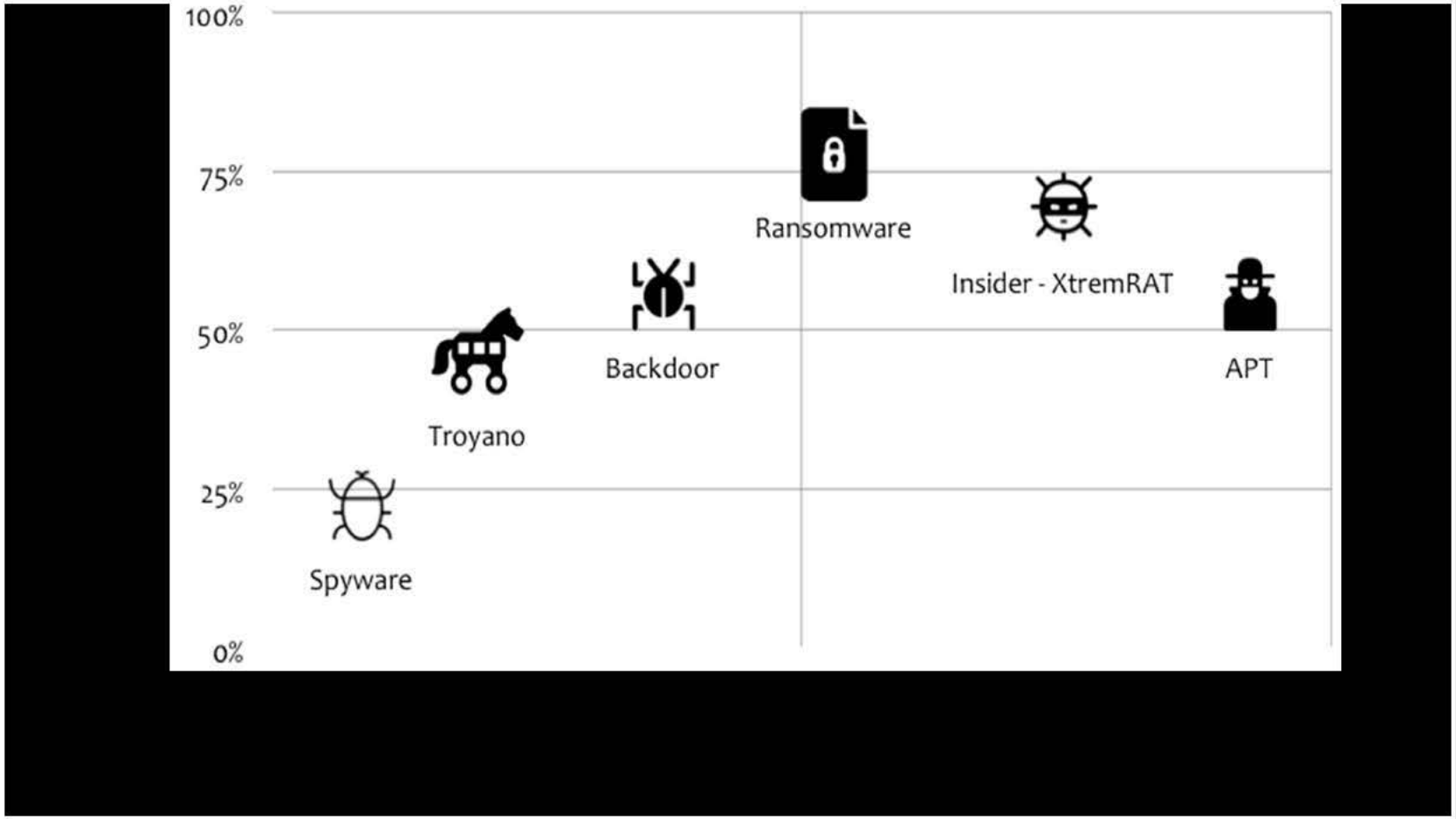
```
!!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
    http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
    1. http://twbers4hmi6dx65f.tor2web.org/32C0D883E1644D0A
    2. http://twbers4hmi6dx65f.onion.to/32C0D883E1644D0A
    3. http://twbers4hmi6dx65f.onion.cab/32C0D883E1644D0A

If all of this addresses are not available, follow these steps:
    1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
    2. After a successful installation, run the browser and wait for initialization.
    3. Type in the address bar: twbers4hmi6dx65f.onion/32C0D883E1644D0A
    4. Follow the instructions on the site.

!!! Your personal identification ID: 32C0D883E1644D0A !!!          !!! IMPORTANT INFORMATION !!!!

All of your files are encrypted with RSA-2048 and AES-128 ciphers.
More information about the RSA and AES can be found here:
    http://en.wikipedia.org/wiki/RSA_(cryptosystem)
    http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

Decrypting of your files is only possible with the private key and decrypt program, which is on our secret server.
To receive your private key follow one of the links:
    1. http://twbers4hmi6dx65f.tor2web.org/32C0D883E1644D0A
    2. http://twbers4hmi6dx65f.onion.to/32C0D883E1644D0A
    3. http://twbers4hmi6dx65f.onion.cab/32C0D883E1644D0A

If all of this addresses are not available, follow these steps:
    1. Download and install Tor Browser: https://www.torproject.org/download/download-easy.html
    2. After a successful installation, run the browser and wait for initialization.
    3. Type in the address bar: twbers4hmi6dx65f.onion/32C0D883E1644D0A
    4. Follow the instructions on the site.
```

1. Ransomware

Tendencias Globales del Cibercrimen

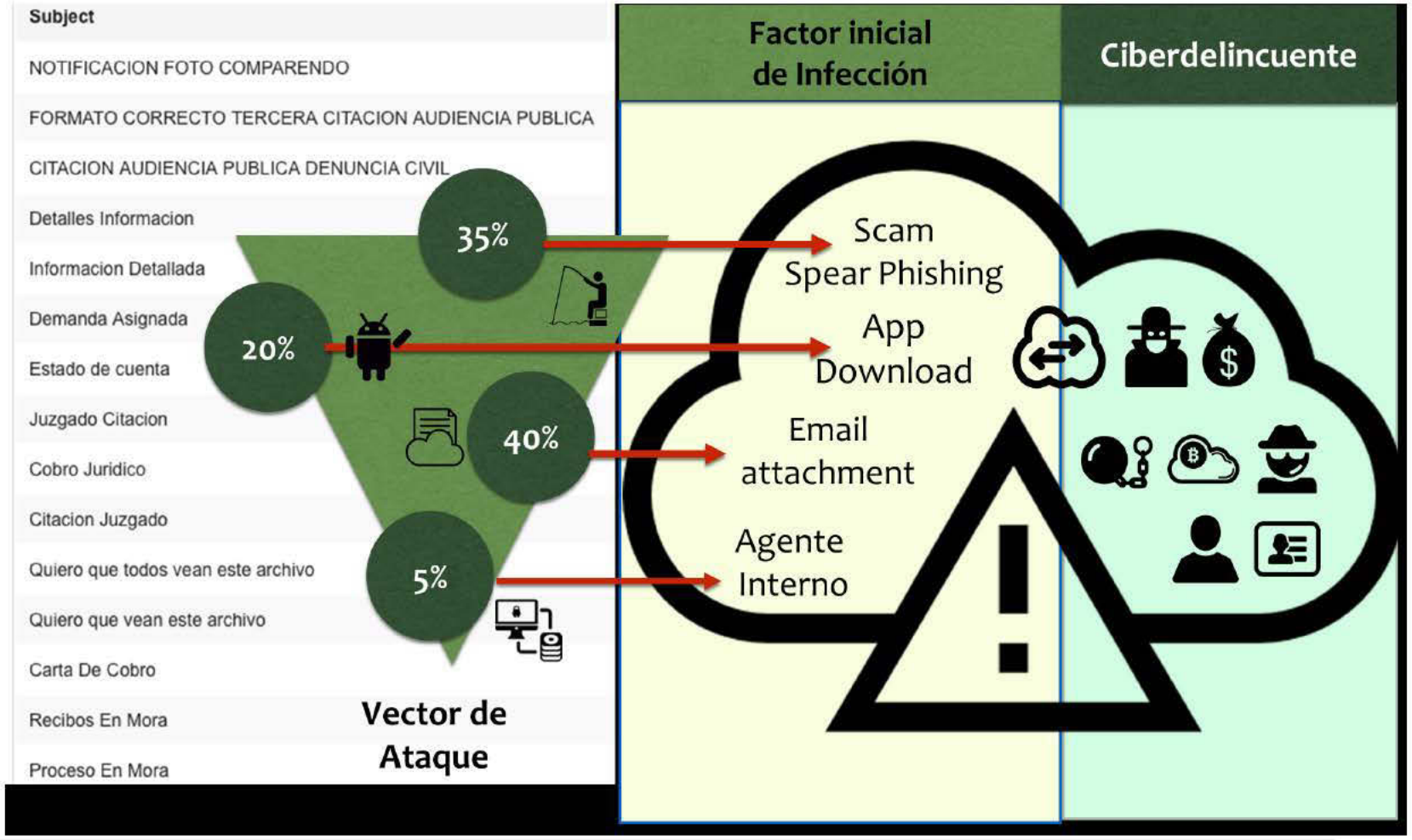
2. Ataques sofisticados de Malware

Tendencias Globales del Cibercrimen



2. Ataques sofisticados de Malware

Tendencias Globales del Cibercrimen



2. Ataques sofisticados de Malware

Tendencias Globales del Cibercrimen

2. Ataques sofisticados de Malware

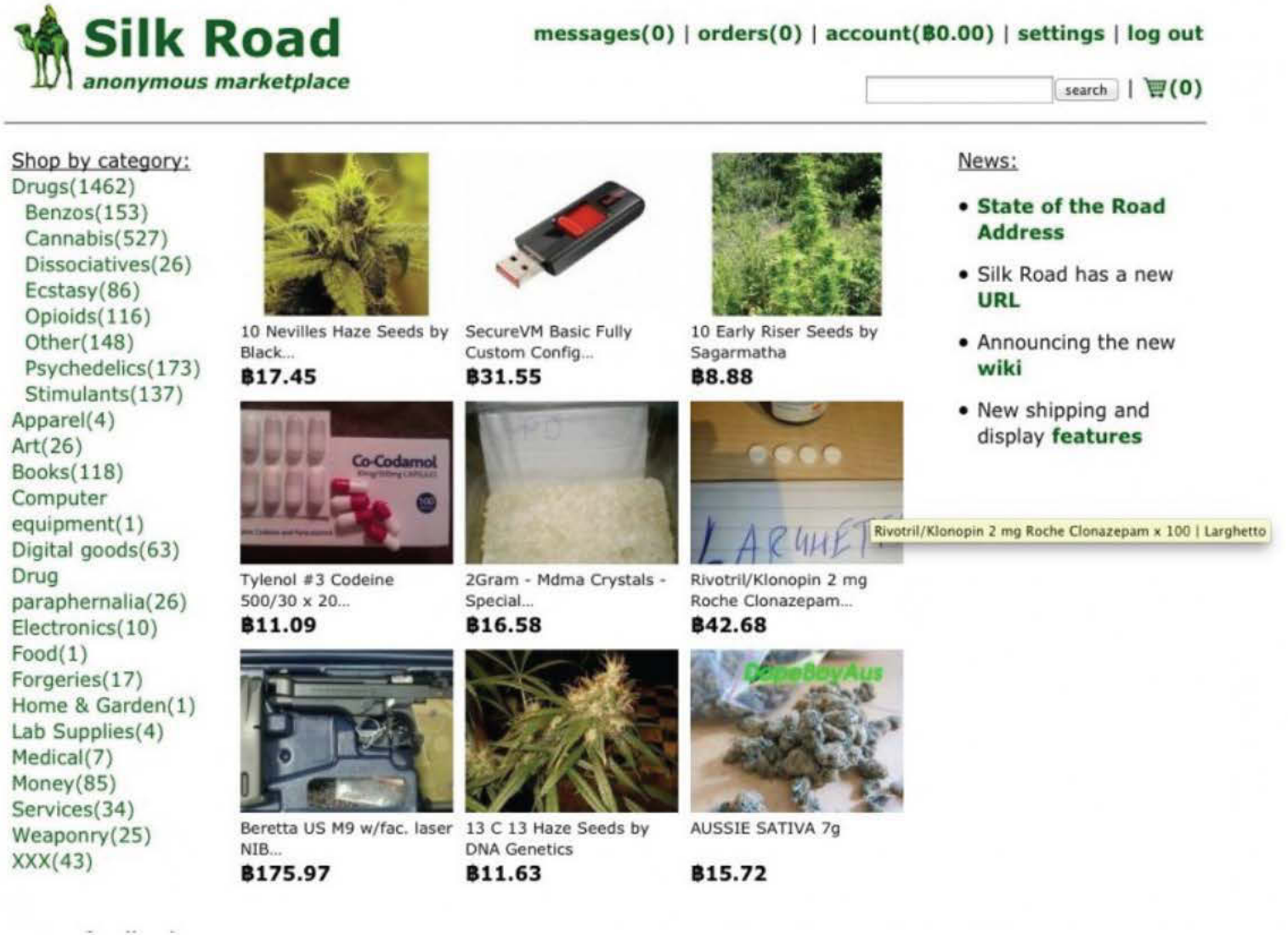
Tendencias Globales del Cibercrimen

2. Ataques sofisticados de Malware

Tendencias Globales del Cibercrimen

3. Mercados Ilegales

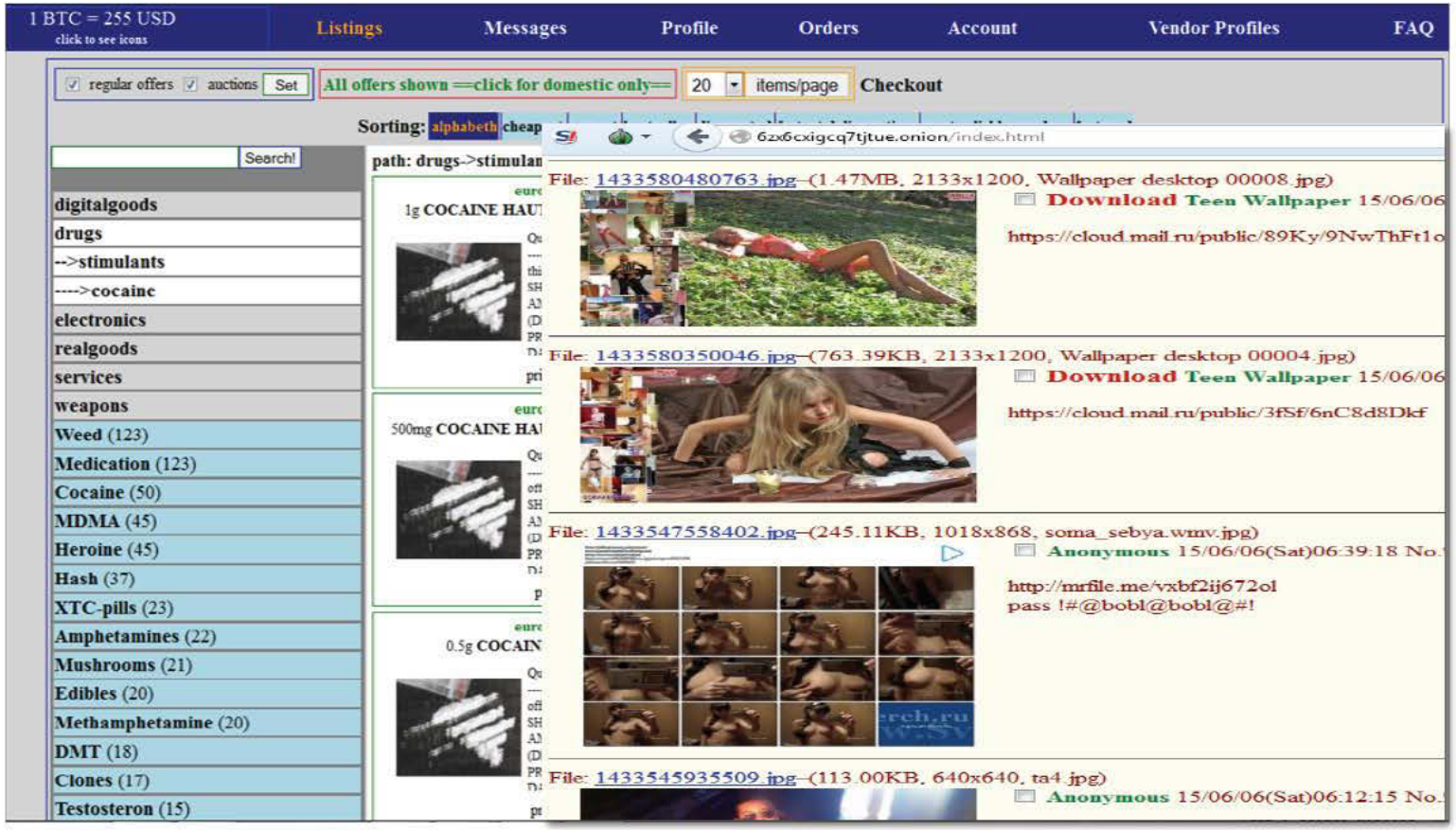
Tendencias Globales del Cibercrimen



3. Mercados Ilegales

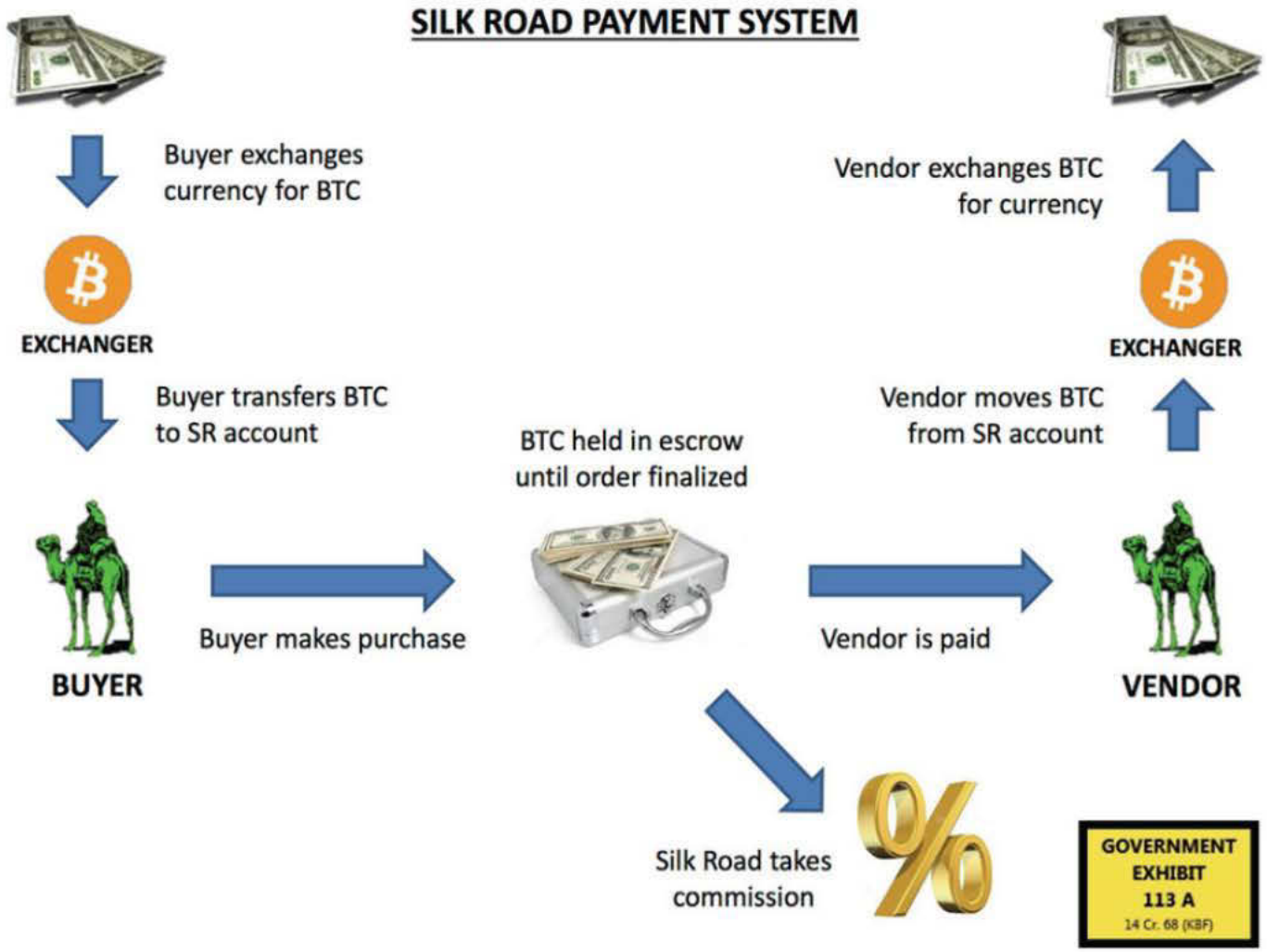
Agora, Pandora, SilkRoad

Tendencias Globales del Cibercrimen



3. Mercados Ilegales

Tendencias Globales del Cibercrimen



4. Internet Profunda

Tendencias Globales del Cibercrimen

4. Internet Profunda

Tendencias Globales del Cibercrimen

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

1. Estructuras Criminales del Cibercrimen

Crimen Organizado 2.0

1. Estructuras Criminales del Cibercrimen

Crimen Organizado 2.0

Condiciones opcionales

- 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 negoci

1. B.E.C. Business Email Compromise

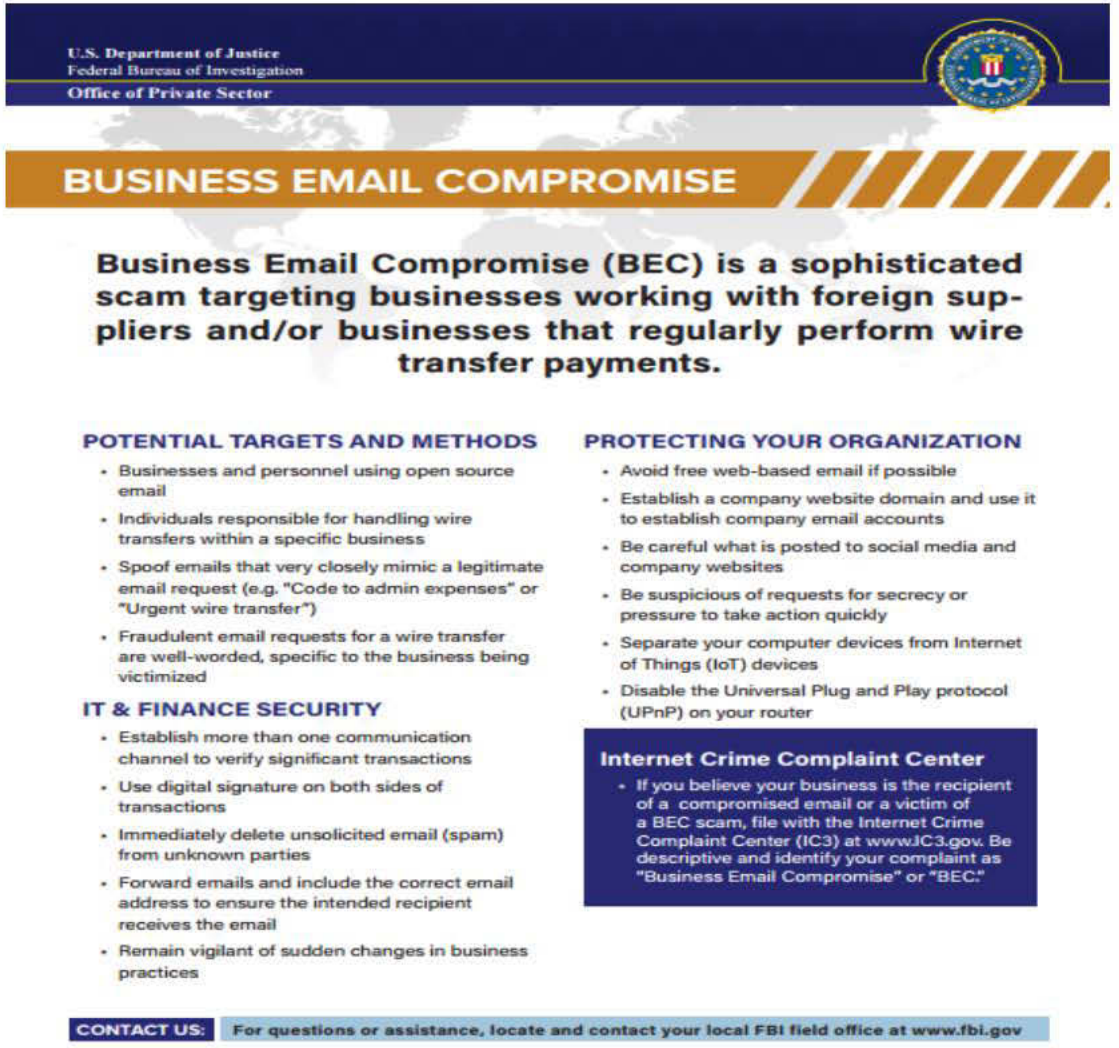
B.E.C.
Business Email Compromise

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

Universidad Externado de Colombia | FACULTAD DE CONTADURÍA PÚBLICA

"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