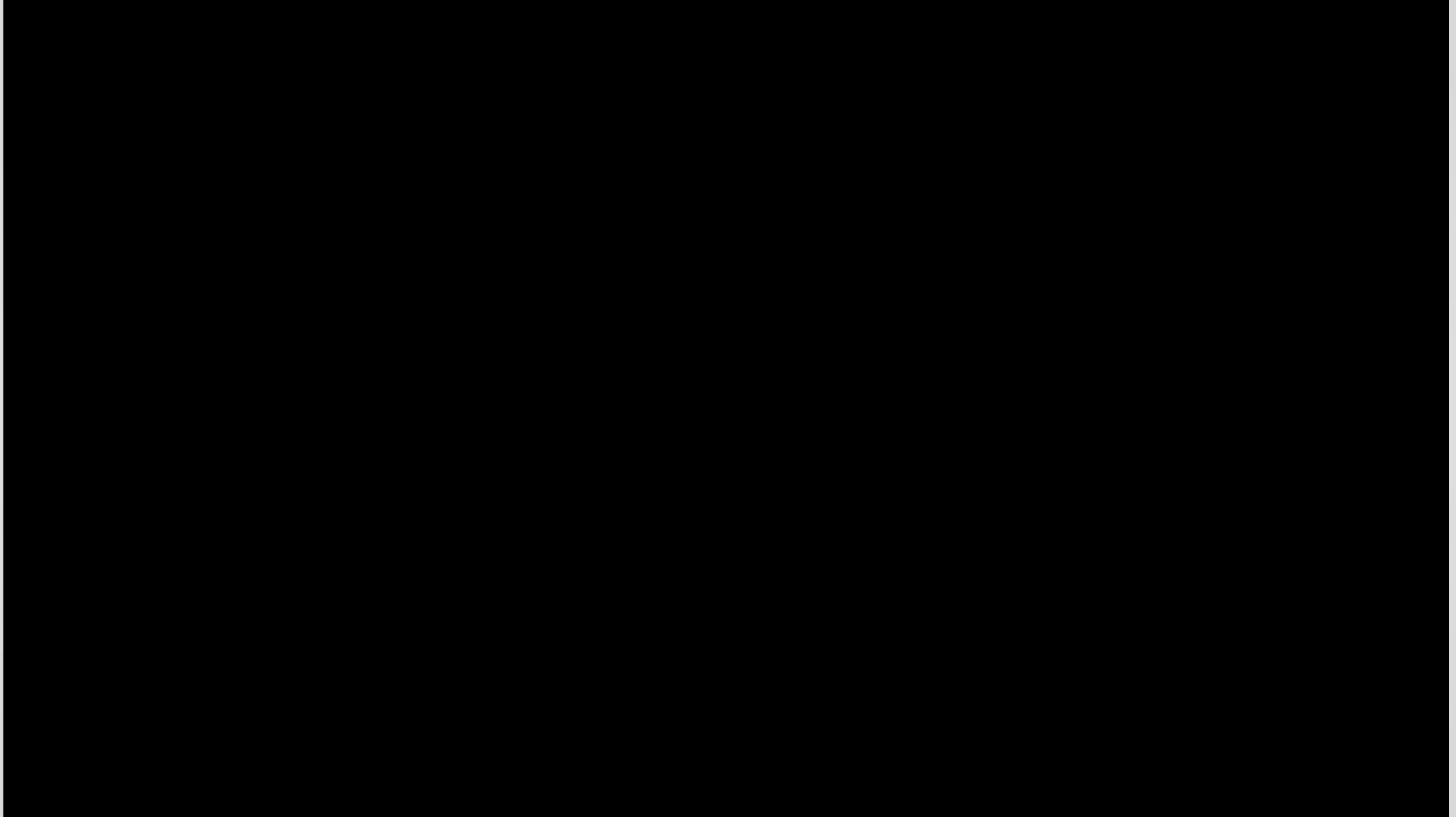
METROPOLITANA DE PEREIRA
SECCIONAL DE INVESTIGACIÓN CRIMINAL

CONTEXTO DEL CIBERCRIMEN EN PEREIRA

Subintendente **PETER VARGAS**
Investigador Cibercrimen
Ingeniero de Sistemas, CHFI,
Desarrollador Backend Python



ACTUALIZACIÓN CONSTANTE EN CIBERSEGURIDAD

https://caivirtual.policia.gov.co

@CaiVirtual

CAPACIDADES – ALCANCE INTERNACIONAL

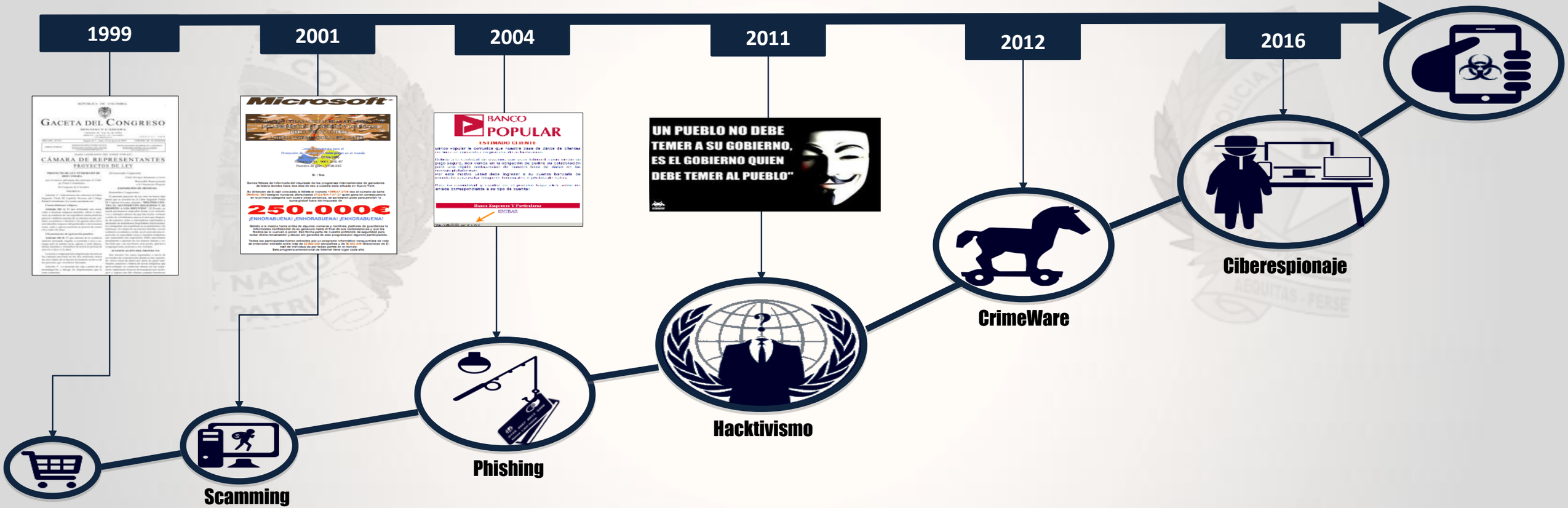
Ley **1582 de 2012** - Acuerdo de cooperación entre Colombia y la oficina Europea de Policía EUROPOL

Agencia Internacional de Cooperación Coreana

Centro Regional para el Cibercrimen en las AMERICAS - Ameripol

Grupo de Trabajo Americano de delitos Tecnológicos de INTERPOL

AMENAZAS – EVOLUCIÓN DEL DELITO



PHISHING

Apple Inc. [US] https://www.icloud.com

¿POR QUÉ ESTOY AQUÍ?

Cancelación Conferencia - Google Chrome

https://outlook.office.com/owa/projection.aspx

Responder a todos | Eliminar Correo deseado | •••

Cancelación Conferencia

A ARISTIDES ALBERTO CABANA GOMEZ<aristides.cabana@mc.net.co>

Responder a todos

Buenos días Peter,

La presente tiene como fin en primera medida desearle éxitos en sus funciones y a la vez informarle que la conferencia programada para el día de hoy fue cancelada.

Atentamente;

ARISTIDES ALBERTO CABANA GOMEZ
Administrador de Red

¿Por qué estoy aquí?

EMAIL SPOOFING

Free online fake mailer with attachments, encryption, HTML editor and advanced settings...

E-mail sent successfully

From Name: ARISTIDES ALBERTO CABANA GOMEZ
From E-mail: aristides.cabana@mc.net.co
To: peter.vargas4942@correo.policia.gov.co
Subject: Cancelación Conferencia
Attachment: Seleccionar archivo No se eligió archivo
Attach another file
Advanced Settings
Content-Type: text/plain text/html Editor
Text:

```
Buenos días Peter,

La presente tiene como fin en primera medida desearle éxitos
en sus funciones y a la vez informarle que la conferencia
programada para el día de hoy fue cancelada.

Atentamente;

ARISTIDES ALBERTO CABANA GOMEZ
Administrador de Red
```

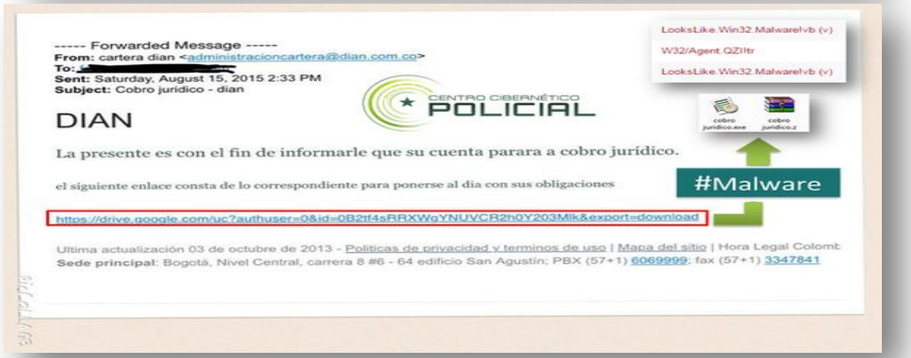
From Name: ARISTIDES ALBERTO CABANA GOMEZ
From E-mail: aristides.cabana@mc.net.co
To: peter.vargas4942@correo.policia.gov.co
Subject: Cancelación Conferencia
Attachment: Seleccionar archivo No se eligió archivo
Attach another file
Advanced Settings
Content-Type: text/plain text/html Editor
Text:

```
Buenos días Peter,

La presente tiene como fin en primera medida desearle éxitos
en sus funciones y a la vez informarle que la conferencia
programada para el día de hoy fue cancelada.

Atentamente;

ARISTIDES ALBERTO CABANA GOMEZ
Administrador de Red
```

MALWARE

Hola como estas espero te encuentres bien, el motivo de mi mensaje es para alertarte de lo que están preparando a tus espaldas gente que dice ser tu amigo solo por envidia quieren atentar contra tu vida, recién ayer estuve en una reunión el cual 2 personas mencionaron tu nombre y tu apellido, yo me sorprendí ya que pues un conocido mio me había hablado de ti y me hablo muy bien
en resumen en mi consciencia no quiero cargar con un muerto, en el momento que ellos hablaban yo grabe la conversación con mi celular acá te la dejo para que la escuches :

http://co.blackberry.com/notasdevozdate07052014



¿Qué sucede si instalo este "archivo"?

El Laboratorio de Informática Forense del Centro Cibernético Policial, analizó detalladamente este archivo, con el fin de identificar sus objetivos.

"¿Por qué el correo me lo envían desde cuentas oficiales?", no lo envían desde cuentas oficiales, utilizan la técnica llamada "Email Spoofing" o "suplantanción de correo electrónico".

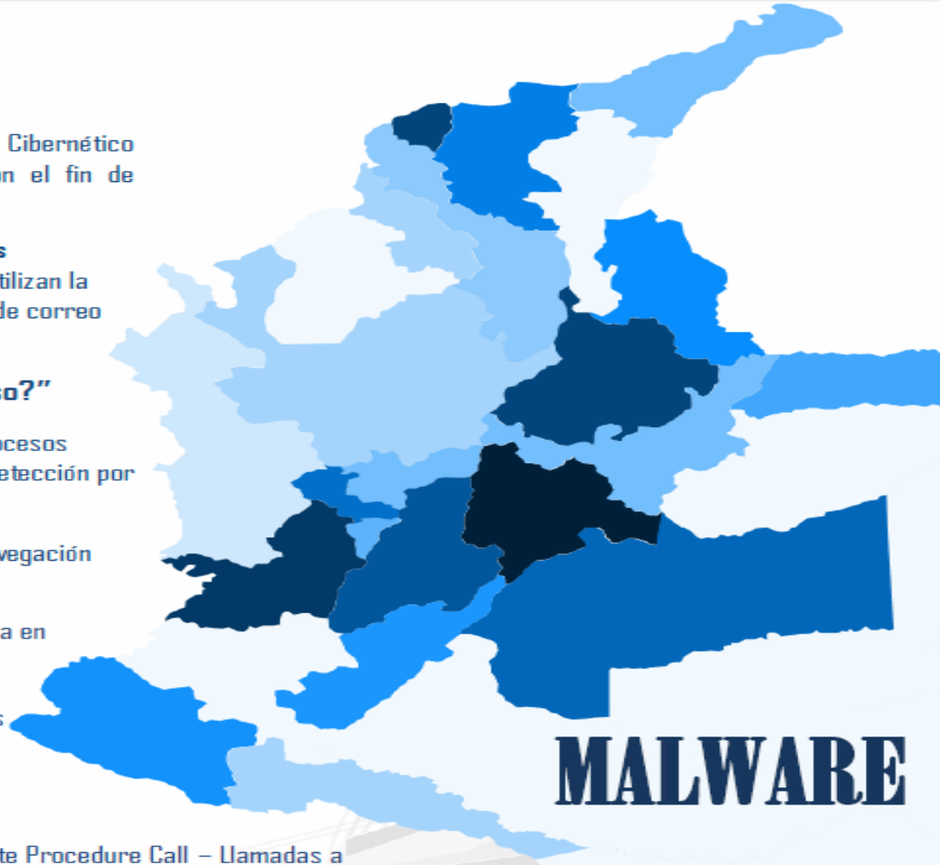
"¿Qué hace este software malicioso?"

En el momento de ser ejecutado se duplican subprocesos legítimos del sistema operativo, para dificultar la detección por parte de los antivirus.

Captura las entradas por teclado y registros de navegación referentes a la banca virtual.

Crea un archivo llamado "server.exe" y lo almacena en la carpeta de las librerías del sistema operativo.

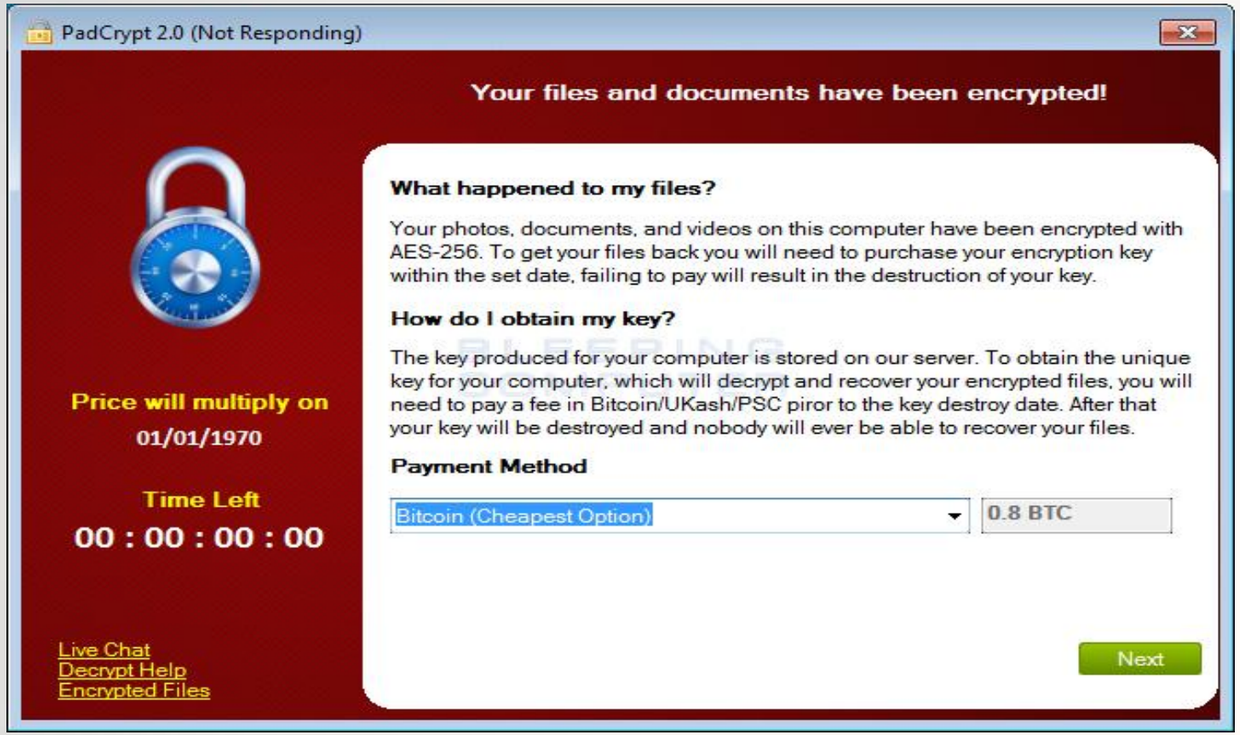
El archivo "server.exe" tiene varias funcionalidades una de ellas es el envío de la información recolectada a un servidor que está previamente configurado por el ciberdelincuente.

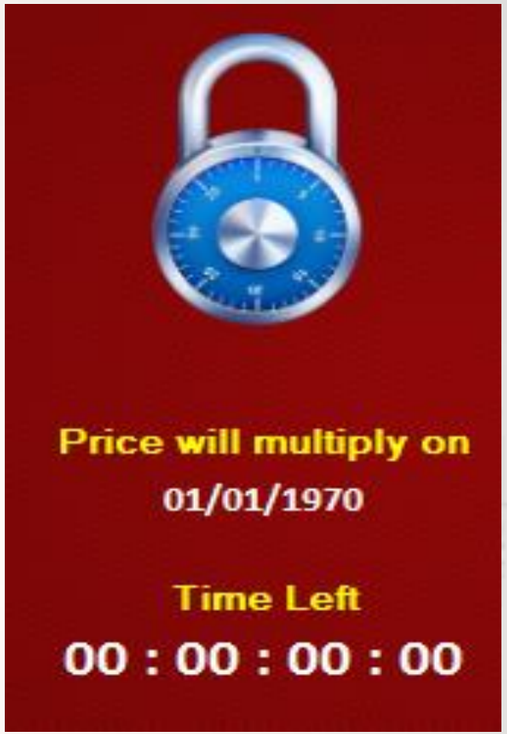


También realiza la apertura de puertos RPC (Remote Procedure Call – Llamadas a Procedimientos Remotos), los cuales permiten el acceso remoto de los ciberdelincuentes a nuestros equipos de cómputo.

Puede ser configurado para supervisar y capturar posibles sesiones de "token Process" que permitiría el acceso a información financiera o confidencial para posibles fraudes ante la Banca Virtual

RANSOMWARE


PadCrypt 2.0 (Not Responding)
Your files and documents have been encrypted!
Price will multiply on
01/01/1970
Time Left
00 : 00 : 00 : 00
What happened to my files?
Your photos, documents, and videos on this computer have been encrypted with AES-256. To get your files back you will need to purchase your encryption key within the set date, failing to pay will result in the destruction of your key.
How do I obtain my key?
The key produced for your computer is stored on our server. To obtain the unique key for your computer, which will decrypt and recover your encrypted files, you will need to pay a fee in Bitcoin/UKash/PSC piror to the key destroy date. After that your key will be destroyed and nobody will ever be able to recover your files.
Payment Method
Bitcoin (Cheapest Option)
0.8 BTC
Next
Live Chat
Decrypt Help
Encrypted Files

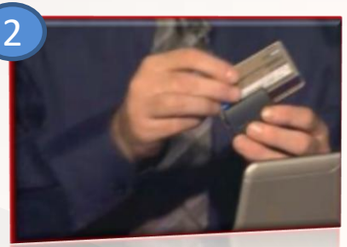

Price will multiply on
01/01/1970
Time Left
00 : 00 : 00 : 00


Payment Method
Bitcoin (Cheapest Option)
0.8 BTC

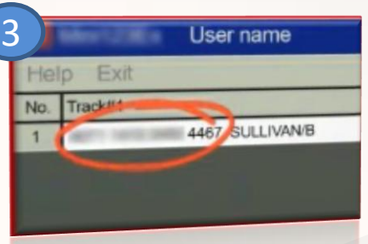
SKIMMING

1

2

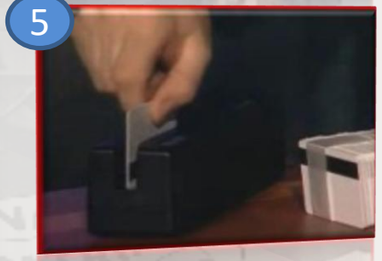


3



4

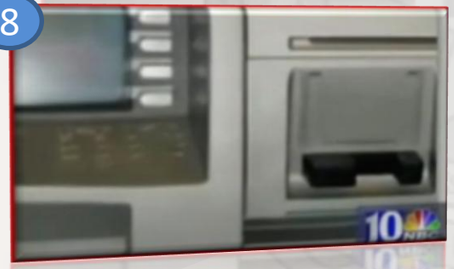
5



6

7

8



9

10

METADATOS

OBTENIENDO EL RASTRO INFORMÁTICO

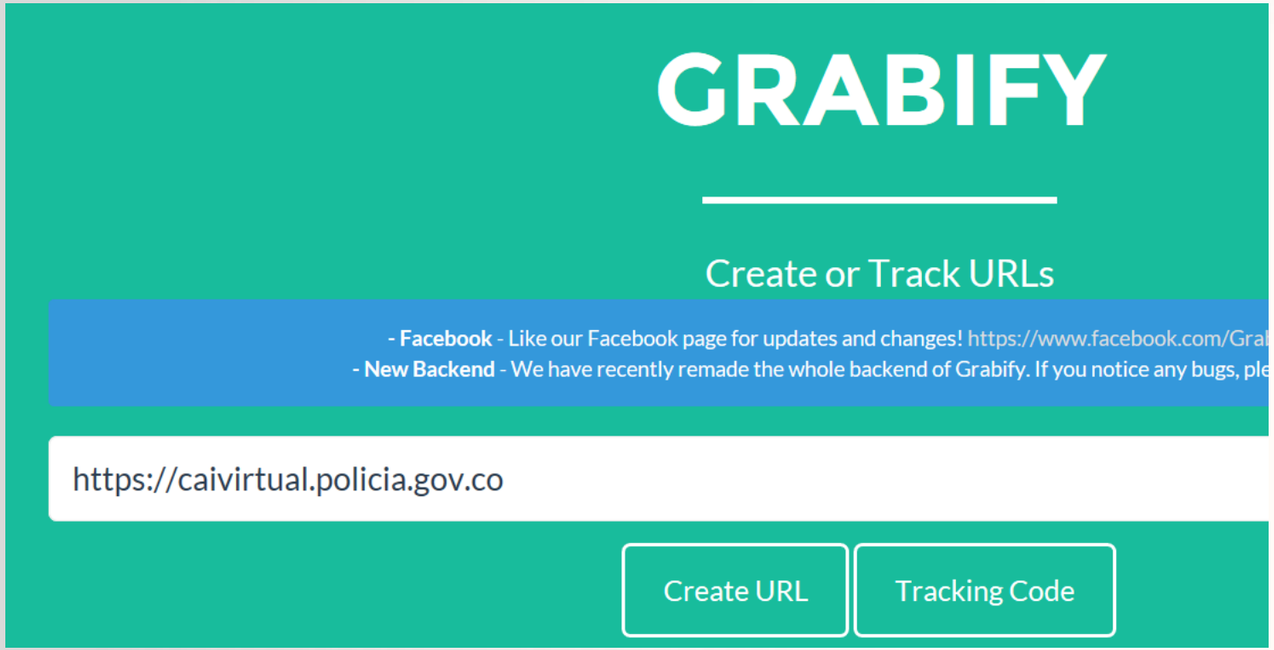
Basic Image Information

Target file: IMG_20181025_181210.jpg

Camera:	Huawei ALE-L23
Lens:	3.7 mm
Exposure:	Auto exposure, Program AE, 1/14 sec, f/2, ISO 1550
Flash:	none
User Comment:	Hisilicon Balong
Date:	**October 25, 2018** 6:12:14PM (timezone not specified) (3 hours, 9 minutes, 49 seconds ago, assuming image timezone of 5 hours behind GMT)
Location:	Latitude/longitude: **4**° 48' 20.6" North, **75**° 43' 2.5" West (4.805735, -75.717351) Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Altitude: 1,363 meters (4,472 feet) Timezone guess from earthtools.org: 5 hours behind GMT
File:	**4,160** × **2,336** JPEG (**9.7** megapixels) 2,361,650 bytes (2.3 megabytes)

http://exif.regex.info/exif.cgi

GRABIFY - https://grabify.link



https://grabify.link

GRABIFY - https://grabify.link

RESULTS: 1

Note: If you have posted your link on Facebook, Twitter, or in a URL shortener, you may see results from various "bots" (BitlyBot, FacebookBot, etc.)

Hide Bots

Date/Time	IP Address	Country	User Agent	Referring URL	Host Name	ISP
2018-10-26 15:30:42	190.9.195.133	Colombia, Medellin	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134	*no referrer*	Cable-Costavision190-9-195-133.une.net.co	EPM Telecomunicaciones S.A. E.S.P.

https://grabify.link

CASO DE ÉXITO

@danielzarama El criterio es "¿es famoso?-Si, ¿es "artista", político o periodista?-Si" entonces es un objetivo para nosotros.

DanielSamperO Sophie Germain

@guitarradavid En Colombia si, en otra nación creo que el FBI ya estaría tocando la puerta a menos que sea un Hacker ruso.

12 ago

Agosto 12

Víctima

Agosto 13

FISCALIA GENERAL DE LA NACION

EPM Bogotá Telecomunicaciones

Agosto 14

Indiciado

Agosto 15

¿Por qué es necesaria una estación de informática forense en software libre para la Policía Nacional?

Prueba Piloto – Metropolitana de Pereira

- Colombia pionero en la implementación en software libre en la informática forense.
- Austeridad en el gasto.
- Apoyo Técnico – Científico a la Administración Justicia.
- Despliegue nacional de estaciones de informática forense.
- Aumento de las capacidades de atención de incidentes informáticos.
- Innovación en la atención e investigación del Cibercrimen.

Innovación y Optimización de Indagación Penal

80% Reducción de Costos

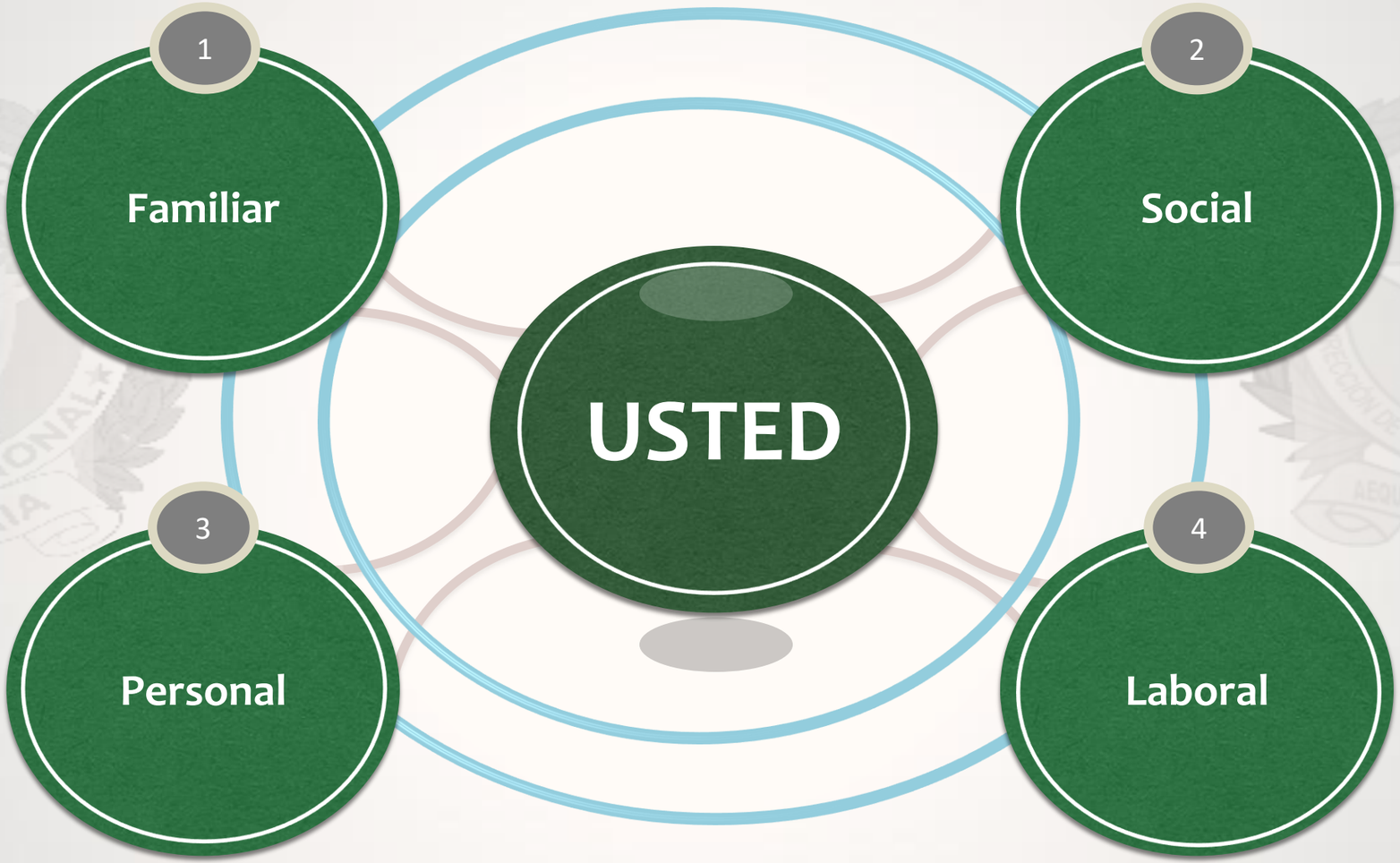
Nuevas técnicas de indagación

Análisis Profundo de Metadatos

Cloud Computing

Monedas Electrónicas

MITIGACIÓN



METROPOLITANA DE PEREIRA
SECCIONAL DE INVESTIGACIÓN CRIMINAL

GRACIAS

Subintendente **PETER VARGAS**
Investigador de Cibercrimen
Ingeniero de Sistemas, CHFI,
Desarrollador Backend Python
(+57) 314 4785159