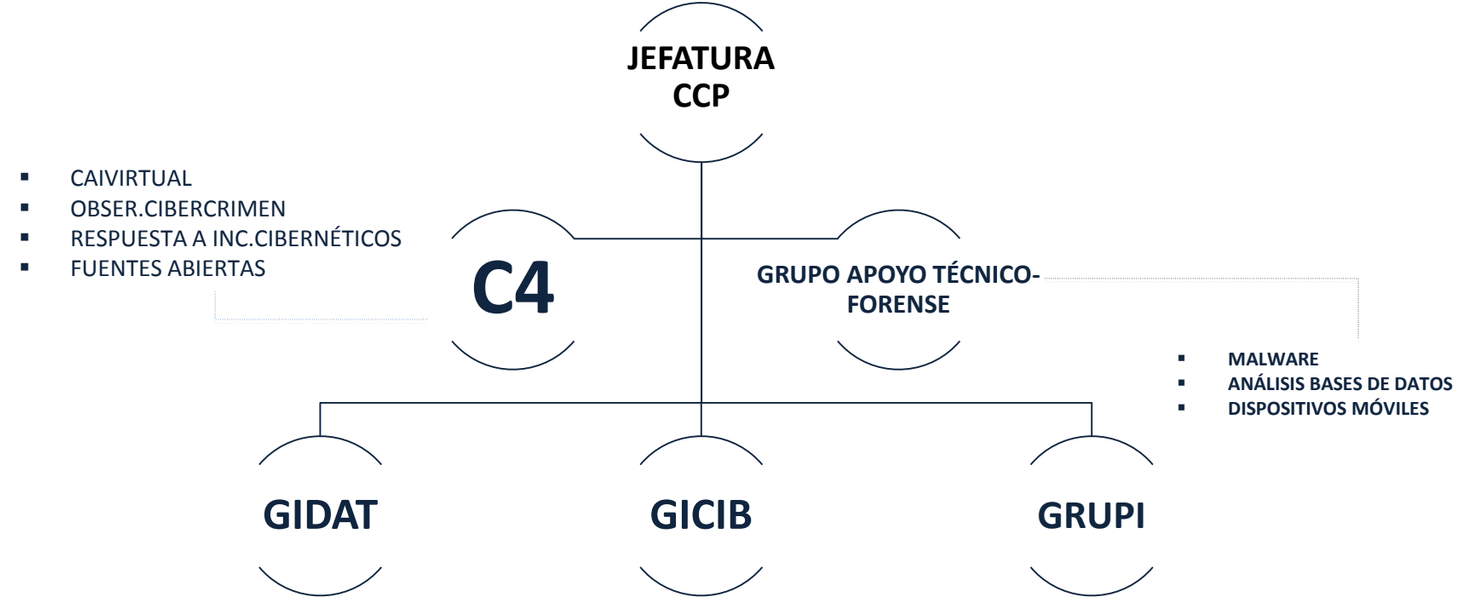
DIRECCIÓN DE INVESTIGACIÓN CRIMINAL E INTERPOL

MODELO DE GESTIÓN PARA LA CIBERSEGURIDAD

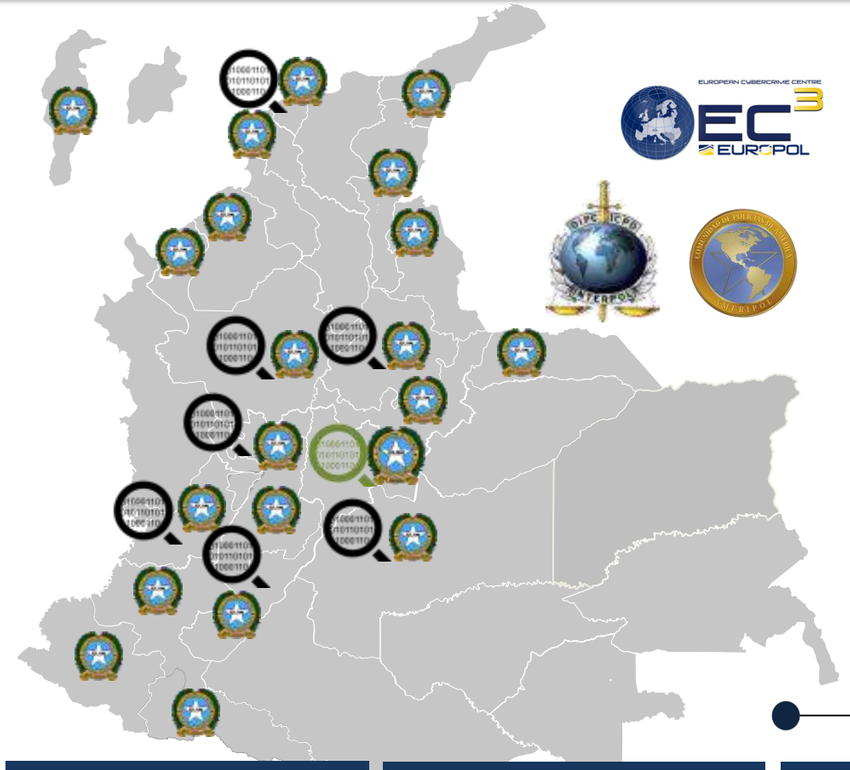
Teniente Coronel FREDY BAUTISTA GARCIA
Jefe Centro Cibernético Policial

Bogotá D.C ., agosto de 2015
www.policía.gov.co

ORGANIGRAMA CENTRO CIBERNÉTICO POLICIAL



CAPACIDADES DEL CENTRO CIBERNÉTICO POLICIAL



COBERTURA Y CAPACIDAD TÉCNICA

- TRATAMIENTO Y ANÁLISIS EVIDENCIA DIGITAL
- ANÁLISIS DISPOSITIVOS MÓVILES

LABORATORIO INFORMÁTICA FORENSE

- BARRANQUILLA
- BUCARAMANGA
- NEIVA
- CALI
- MEDELLÍN
- MANIZALES
- VILLAVICENCIO

UNIDADES DE INVESTIGACIÒN TECNOLÓGICAS

LAB. SECCIONALES DE INFORMÁTICA FORENSE

PUNTO DE CONTACTO RED 24/7 DEL G8

PRESIDENCIA DEL GRUPO DE TRABAJO AMERICANO DE CIBERCRIMEN INTERPOL

PRESENCIA EC3 EUROPEAN CYBERCRIME CENTER EUROPOL

CAI VIRTUAL
www.ccp.gov.co

- PRIMER SERVICIO DE ASISTENCIA PERSONALIZADA ONLINE
- 8.164 ALERTAS EN REDES SOCIALES
- 23.000 SEGUIDORES EN REDES SOCIALES
- CONTACTO CON GRUPOS EXPERTOS EN CIBERSEGURIDAD
- 122.736 USUARIOS DEL SERVICIO EN EL 2015

SITIO WEB CIBERSEGURIDAD

WWW.CCP.GOV.CO

LABORATORIOS ESPECIALIZADOS

APLICACIONES MÓVILES

PROTECTIO | CAI VIRTUAL | APP ANTIRROBO

DENUNCIA EN LINEA

MODELO OPERACIONAL EN MATERIA DE CIBERCRIMEN

FUENTE → Noticia Criminal
Ley 1273 de 2009

- CAI Virtual -- CCP
- CSIRT sectoriales COLCERT
- Ciudadano
- CCOC

FISCALIA GENERAL DE LA NACION

Programa metodológico

Art. 207 Ley 906/2004

DIJIN

Ordenes de:

- ❑ Captura
- ❑ Allanamiento
- ❑ Incautación de evidencia digital

PMU

- ❑ Coordinación
- ❑ Comando y control – C4
- ❑ Monitoreo y difusión
- ❑ Neutralización de la amenaza

COMPONENTES

A CENTRO CIBERNÉTICO POLICIAL

- ❑ Realiza procedimiento operativo
- ❑ Incauta EMP y EF en el lugar de los hechos
- ❑ Judicialización de responsables
- ❑ Realiza peritajes en informática forense
- ❑ Presentación de informes ante la F.G.N.

B

EUROPOL (EC3) | **INTERPOL** | **FBI** | **AMERIPOL**

- ❑ Verificación de objetivos en común
- ❑ Verificación de antecedentes del objetivo
- ❑ Apoyo técnico científica
- ❑ Acciones judiciales conjuntas en países afectados

C

COLCERT

- ❑ Reportes de ataques
- ❑ Monitoreo 24/7 a redes de telecomunicaciones
- ❑ Alertas a CSIRT sectoriales - CCOC

D

CCOC

- ❑ Activación
- ❑ Reporte de incidentes informáticos a P.J. – CENTRO CIBERNÉTICO POLICIAL
- ❑ Detección de amenazas contra la infraestructura crítica del país

A B C D
AMENAZA POR PARTE DE OTRO ESTADO O PAÍS

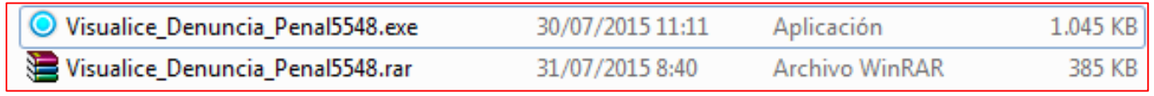
A B C
AFECTACIÓN AL GOBIERNO

A B C
AFECTACIÓN SECTORIAL

A B
AFECTACIÓN AL CIUDADANO

PERIMETROS DE ACTUACIÓN

MODELO DE GESTIÓN CASO PRÁCTICO



Reporta al CAIVIRTUAL caso **SPAM**

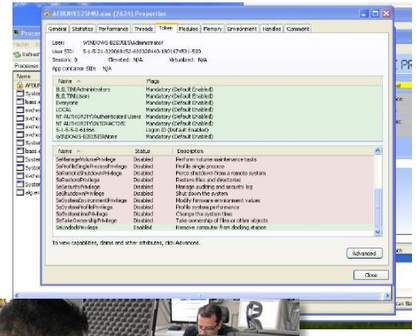
Al verificar es un **PHISHING** que usurpa la identidad de la **F.G.N.**

FISCALÍA GENERAL DE LA NACIÓN

Radicado No. 2234109381000
Oficio No. 30-07-2015
Pagina 1 de 1
DFGN-GN
CITACION UNICA
BOGOTA D.C
La FISCALIA GENERAL DE LA NACION y La doctora Martha Oliva Pineda Correa, en su condiciÃ³n de Fiscal 85 Seccional Delegada ante los Jueces Penales del Circuito de la ciudad de BogotÃ¡, Por medio del presente documento le informan:
Que la la resoluciÃ³n de acusaciÃ³n en su contra ha sido determinada y en consecuencia **solicitamos su presencia en este despacho sin falta el dia JUEVES 24 DE SEPTIEMBRE DE 2015, A LAS 3:30PM,** con el fin de rendir indagatoria por los cargos de Hurto agravado en primera persona en el caso contra el seÃ±or PEDRO DEL CARMEN BENAVIDES. **SU ASISTENCIA ES OBLIGATORIA (recuerde llevar su documento de identidad).**
Para ver mas informacion acerca su proceso y fecha de la citacion visualice el siguiente archivo en linea:
http://fiscalia.gov.co/procesos/bogota/2234109381000

REF:
DENUNCIA PENAL
Punible:HURTO AGRAVADO(Ley 599 del aÃ±o 2000 artÃculos 239 a 241
Ref: CitaciÃ³n Diligencia de Descargos
31/07/2015 04:44:14

Al dar clic sobre el enlace se descarga un *.rar



Se envía al laboratorio para su análisis

Resultado del análisis

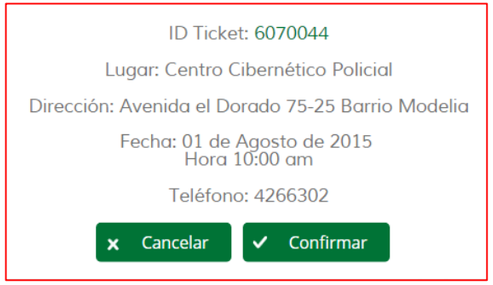
Se generan alertas a la ciudadanía

Se toma contacto con el Web master del sitio afectado para mitigar el incidente

Gerentes de empresas reportan caso de SPEAR PHISHING

CAIVIRTUAL toma contacto con las víctimas

Registro de incidentes en www.ccp.gov.co



Recepción personalizada de denuncias - CCP

JULIO 31 2015 10:00 AM

JULIO 31 2015 10:15 AM

JULIO 31 2015 10:45 AM

JULIO 31 2015 03:45 PM

AGOSTO 1 2015 09:00 AM

DESPLIEGUE OPERATIVO INTERNACIONAL

1 Pornografía infantil

- Operación Deplation W3 → Siena 1130365-7-1
- Operación Pacifier → Siena 1126113-15-1 (DD)
- Operación Latvia → Siena 1106724-3-1
- Canadá → Siena 1144176-1-1
- Operación Red Eclipse → Siena 1126430-690-1

2 Fraude en Línea

- Operación Nosema → Siena 1104575-2-1

FINALIZADA Operación Action Day Fraud → Siena 1116641-14-1

3 Dark Web

- Operación ONYMOUS → Siena 1101411-188-1

FINALIZADA Operación DARKCODE → Siena 1139211-1-1

4 Propiedad Intelectual on Line

- Operación IOS VI → Siena 1101446-14-1

Malware Bancario

A través del EC3 se puede acceder a las muestras de Malware que se analiza en EUROPOL.

Amenazas

- DYRE → Siena 1132257-1-1 y 1128614-10-1
- CARBANAK → Siena 1125900-1-1
- TIMBA (Op Nosema) → Siena 1104575-2-1
- DRYDEX Información de inteligencia España
- CORKOW Botnet Rusa Información Inteligencia

DESPLIEGUE OPERATIVO INTERNACIONAL

Mediante Operación DARKODE cerramos un espacio que fue usado por cibercriminales

viernes, 17 de julio de 2015. La DIJIN e INTERPOL de la Policía Nacional Colombia y otras agencias de Ley a nivel mundial, adelantaron esta Operación en contra del foro de hackers en la red.

Centro Cibernético @CaiVirtual · 17 jul.
Como resultado de la operación DARKODE, se lograron 28 capturas y 37 allanamientos (darkode.com)
Policía de Colombia, DIJIN, FSE - DIJIN y Centro Cibernético

1

Dirección de Investigación Criminal e INTERPOL

www.ccp.gov.co

Avenida el Dorado N° 75-25
Teléfono: 426 63 01

Bogotá D.C., agosto de 2015