



VIII JORNADAS SOBRE PREVENCIÓN Y REPRESIÓN
DEL BLANQUEO DE CAPITALES

COMPROMISO CON LA TRANSPARENCIA

Castellón, 7 y 8 de abril de 2022

Los nuevos riesgos derivados de la digitalización. Las criptomonedas

José García, Comisario jefe de la Brigada Central de fraude informático



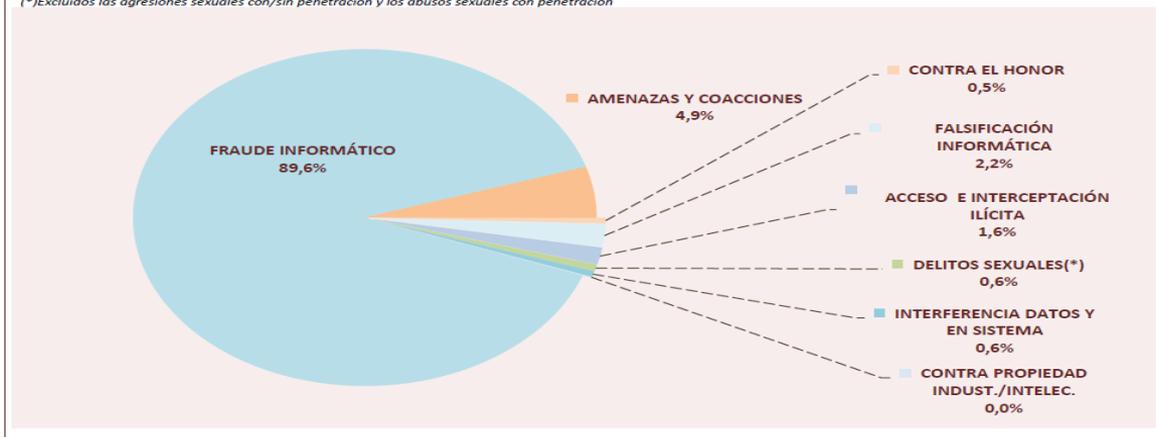




>> **4.1. Evolución de hechos conocidos por categorías delictivas**

HECHOS CONOCIDOS	2016	2017	2018	2019	2020
ACCESO E INTERCEPTACIÓN ILÍCITA	3.243	3.150	3.384	4.004	4.653
AMENAZAS Y COACCIONES	12.036	11.812	12.800	12.782	14.066
CONTRA EL HONOR	1.546	1.561	1.448	1.422	1.550
CONTRA PROPIEDAD INDUST./INTELEC.	129	121	232	197	125
DELITOS SEXUALES(*)	1.231	1.392	1.581	1.774	1.783
FALSIFICACIÓN INFORMÁTICA	3.017	3.280	3.436	4.275	6.289
FRAUDE INFORMÁTICO	70.178	94.792	136.656	192.375	257.907
INTERFERENCIA DATOS Y EN SISTEMA	1.336	1.291	1.192	1.473	1.590
Total HECHOS CONOCIDOS	92.716	117.399	160.729	218.302	287.963

(*)Excluidos las agresiones sexuales con/sin penetración y los abusos sexuales con penetración



2016	2017	2018	2019	2020
4,6%	5,7%	7,5%	9,9%	16,3%



Criptovalores



Entre 0,5 y 3 por ciento con tendencia a la baja (según INE 0,87% del PIB se considera actividades ilícitas)



Características facilitadoras

Anonimato

No bloqueo incautación de monederos privados (salvo detección registro)

Irreversibilidad y rapidez de las operaciones

Escasa regulación (trasposición V directiva, sujetos obligados exchanges y gestores de monederos)

Renovación generacional en las organizaciones delictivas



Utilización de los criptoactivos con fines ilícitos

1. Pago de servicios delictivos. Pago entre delincuentes (C2C)
2. Mecanismos de fraude
3. Blanqueo de fondos de origen delictivo



1. Pago de servicios delictivos

- Ramsonware (ej. Wannacry 2017)
- Mercados dark web: numeraciones de tarjetas, aplicaciones con malware malicioso, armas, drogas, documentaciones falsificados, información sensible...
- Ciberextosiones

Actuaciones:

- Trazabilidad de las operaciones a través de la cadena blockchain para identificar al autor. Necesidad de software de trazabilidad
- Análisis de operaciones
- Intervención de los criptovalores en Exchanges



Buenos días.

Tengo malas noticias para usted.

Mi virus infectó su dispositivo a través de un sitio web para adultos que visitó recientemente.

Este software me da acceso a todos los controladores de sus dispositivos.

He cargado toda su información, los datos, las fotos e el historial de navegación en mis servidores. Tengo acceso a todos sus mensajeros, las redes sociales, el correo electrónico, el historial de chat y la lista de contactos.

Mi virus actualiza constantemente sus firmas y, por lo tanto, permanece invisible para el software antivirus.

Mientras he recopilado la información sobre usted, he **descubierto** que **eres un gran amante de los sitios para adultos y otras cosas divertidas**.

Realmente le encanta visitar sitios pornográficos y ver los videos emocionantes para obtener un montón de placer.

Bueno, **puede grabar algunas de sus escenas sucias y editar videos que vi muestran masturbándose y llegando al orgasmo**.

Si tiene dudas, **puedo hacer unos pocos clics y todos sus videos estarán disponibles para todos los que conoces**.

También puedo publicar toda su correspondencia, fotos personales y todos sus datos secretos en Internet.

Podría arruinar su reputación para siempre.

Supongo que usted no quiere que esto suceda, dados los detalles del video que vi encanta ver(entiende perfectamente a lo que me refiero), ya que este será un verdadero desastre para usted.

Resolvámoslo así: **usted me transfiere \$ 1200 (en equivalente del bitcoin al tasa de cambio en el momento de la transferencia), y tan pronto como se reciba la transferencia, inmediatamente eliminaré toda esta suciedad.**

(Si no sabe cómo hacerlo, escriba en el cuadro de búsqueda de Google: "Comprar bitcoins").

También prometo a desactivar y eliminar todo el software malicioso de sus dispositivos.

Siempre mantengo mi palabra.

Mi billetera Bitcoin para el pago: bc1qwgsecq4qxz2zfec8kccqwxyn5l3n67a23ggrcm

Tiene 50 horas (un poco más de 2 días) para completar este pago.

Si no enviará el dinero, su video y todos sus datos se publicarán en Internet para todo el mundo y sus familiares próximos.

Arruinaré su reputación para siempre.

No trate de encontrarme.

No intente ponerse en contacto con la policía y otros servicios de seguridad, de lo contrario sus datos se publicarán.

Yo se muchos sus secretos.

Considera su reputación!



Code unité : 0437	Nmr : 01574	Año : 2022	CONVOCACIÓN	Nmr : pièce	N°feuillelet:1/1
-------------------	-------------	------------	--------------------	-------------	------------------

A su atención

Una citación para ti :

A petición del Sr. **MARC DE MESMAEKER**, Comisario General de la Policía Federal, elegido para el cargo de Director de Europol, le enviamos esta citación.
 La citación por un agente de la policía judicial está prevista en el artículo 390-1 del Código de Procedimiento Penal. Equivale a una citación para comparecer ante el Tribunal y la decide el Director General de la Policía.

IDENTIDAD DEL CULPABLE	PERSONA CONVOCADA POR CORREO ELECTRÓNICO	CURSO DE PROCEDIMIENTO
------------------------	--	------------------------

En virtud de lo dispuesto en el artículo 372 del Código Penal se establece : " Cualquier atentado al pudor, cometido sin violencia o amenazas a la persona o con la ayuda de la persona de un niño de cualquier sexo, menor de 16 años, será reprimido con reclusión."

Estamos tomando acciones legales contra usted poco después de una incautación informática de la Ciberinfiltración para :

- Pornografía Infantil
- Exhícionismo
- Pedofilia
- Ciberpornografía

Para su información, la Ley 390-1 del Código Procesal Penal, de marzo de 2007, endurece las penas cuando las proposiciones, las agresiones sexuales o las violaciones se hayan cometido a través de Internet.

Usted cometió el delito después de haber sido blanco en Internet (sitio de anuncios), la visualización de videos de pornografía infantil, fotos/videos de desnudos de menores, fueron grabados por nuestro ciberpolicia y constituyen una prueba de sus delitos.

En aras de la confidencialidad, le enviamos este correo electrónico, se le solicita que se haga oír por correo electrónico escribiendo sus justificaciones para que sean examinadas y verificadas a fin de evaluar las sanciones, esto dentro de un plazo estricto de 72 horas. Transcurrido este plazo, nos veremos obligados a transmitir nuestro informe al señor FRANCISCO PARDO PIQUERAS, Director General de la Policía, para que establezca una orden de detención, y se proceda a su inmediata detención por la policía más cercana a su domicilio, y se le inscriba en el registro nacional de delincuentes sexuales. Su expediente también se enviará a las asociaciones contra la pedofilia y a los medios de comunicación para su publicación como persona fichada.

Atentamente,

COMISARIO GENERAL DE POLICIA JUDICIAL
 DIRECCIÓN GENERAL DE LA POLICÍA - ESPAÑA
 Av. de Pío XII
 28016 Madrid

PONGASE EN CONTACTO CON NOSOTROS AQUÍ: comisario.general.de.policia.judicial@europa.com



Modelo de **Nota de rescate** detectada en los 8 casos (_HOW_TO_DECRYPT.txt):

Your network has been breached and all data were encrypted.
Personal data, financial reports and important documents are ready to disclose.

To decrypt all the data and to prevent exfiltrated files to be disclosed at
<http://hiveleakdbtnp76ulyh152eag8c6tyc3xw7ez7iqy6wc34gd2nekazyd.onion/> ← URL donde HIVE publica datos sustraídos a las víctimas
you will need to purchase our decryption software.

Please contact our sales department at:
<http://hivecust6vhkztbqgdnkks64ucehqacqe3di13gyrrpdp57zoq3ooqd.onion/> ← URL donde HIVE negocia el pago con las víctimas

Login: 
Password: 

To get an access to .ONION websites download and install Tor Browser at:
<https://www.torproject.org/> (Tor Browser is not related to us) ← Instrucciones para acceder a TOR

Follow the guidelines below to avoid losing your data:

- Do not modify, rename or delete *.key.bcksz files. Your data will be undecryptable.
- Do not modify or rename encrypted files. You will lose them.
- Do not report to the Police, FBI, etc. They don't care about your business. They simply won't allow you to pay. As a result you will lose everything.
- Do not hire a recovery company. They can't decrypt without the key. They also don't care about your business. They believe that they are good negotiators, but it is not. They usually fail. So speak for yourself.
- Do not reject to purchase. Exfiltrated files will be publicly disclosed.

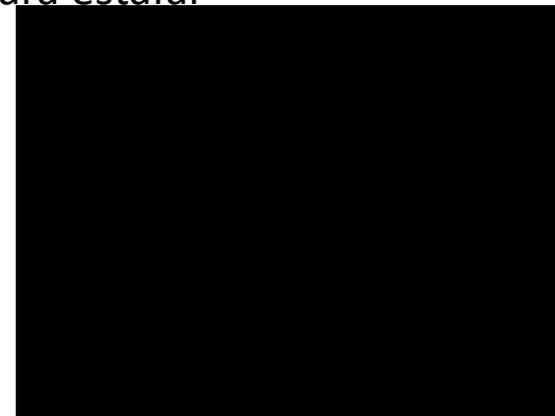
Extorsión a las víctimas plasmada en una serie de advertencias de obligado cumplimiento.
En caso de no aplicarlas los ciberatacantes amenazan con la pérdida de los datos cifrados y con la publicación de información sustraída.

Credenciales únicas para cada víctima



2. Mecanismo de fraude

- Inversiones online de criptovalores
- Esquema Ponzi
- Compra de criptovalores nuevos: sube precio y vende
- Exchanges sin garantías o directamente falsos
- Monederos de aplicaciones generados únicamente para estafar
- Criptojacking
- Deep fake





3. Blanqueo de fondos de origen delictivo

- Motivos: anonimato, rapidez operaciones, desregularización, transnacional y cada vez mayor aceptación
- Proceso: dinero fiat ilegítimo → cripto → diversificación → regreso circuito
(actualmente también está siendo utilizado para almacenar y para staking)
- Actores transacciones criptoactivos: minería, exchanges, local traders, cajeros, proveedores de servicios – bienes y tarjetas de criptoactivos



INTERVENCIÓN DE CRIPTOVALORES

Oficiando a los exchanges

Claves públicas y privadas

Frase semilla

Monedero frío generado (traspaso de fondos)

“Cuenta de depósitos y consignaciones judiciales”



DIFICULTADES ACTUACIÓN POLICIAL

Irreversibilidad y rapidez de las operaciones

Múltiples jurisdicciones

Poca información

Algunas criptos son muy complicadas de rastrear

Utilización de mixers-swapers

Constante evolución

Soluciones: herramientas tecnológicas, formación y cooperación

internacional



MUCHAS GRACIAS



José García Serrano
Comisario
Brigada Central de Fraude Informático
Unidad Central de Ciberdelincuencia
Tfno.: 915822360

POLICIA 
NACIONAL