FORO INTERNACIONAL SOBRE DELITOS FINANCIEROS

Teniente Coronel FREDY BAUTISTA GARCÍA
Jefe Centro Cibernético Policial

FORO INTERNACIONAL SOBRE DELITOS FINANCIEROS

Teniente Coronel FREDY BAUTISTA GARCÍA
Jefe Centro Cibernético Policial

Tendencia actual del cibercrimen

- Ransomware — Secuestro de información
- CryptoLocker
- Malware para móviles
- Deep Web — Internet profundo / oscuro
- Bulletproof — Servidores a prueba de balas
- Bitcoin — Moneda virtual
- Botnet — Red de computodores zombies
- Malware financiero


Your personal files are encrypted.
Your personal files are encrypted.
Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.
Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.
You only have 72 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.
Press 'View' to view the list of files that have been encrypted.
Press 'Next' to connect to the secret server and follow instructions.
WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.
View
71:59:07
Next >>
can open it and use copy-paste for address and key.

Your personal files are encrypted!

Private key will be destroyed on
9/24/2013
6:21 PM

Time left

54 : 15 : 15

Your important files **encryption** produced on this computer: photos, videos, documents. etc. **Here** is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt filesyou need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **100 USD / 100 EUR /** similar amount in another currency.

Click <Next> to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by the server.

From: info@[redacted]al.co
To: j[redacted]@hotmail.com
Subject: NOTIFICACION REPORTE NEGATIVO DATACREDITO
Date: Wed, 29 Jul 2015 13:15:25 -0500

CENTRO CIBERNÉTICO POLICIAL

Mi DataCrédito
Su Historia de Crédito con alertas

Usted tiene un nuevo aviso en su Historia de Crédito.

- Cambio en el saldo en mora de una obligación o cuenta en su historia de crédito. El saldo en mora de la obligación o cuenta número *****3899

Una vez la usted **haya pagado la obligación**, el dato **negativo permanecerá por el doble del tiempo que estuvo en mora**, contado a partir de la fecha de pago, si la mora fue inferior a dos años.
Si la mora fue igual o superior a dos años, tendrá una permanencia de cuatro años, contados a partir de la fecha de pago.

Para consultar el valor a pagar adjunto le enviamos su factura

Ransomware

Cifras Ley 1273 de 2009 --> 2015

Acceso abusivo a sistema informático	**1165**
Obstaculización ilegítima de S.I.	**6**
Interceptación de datos informáticos	**20**
Daño informático	**29**
Uso de software malicioso	**10**
Suplantación de sitios Web	**82**
Circunstancias de agravación punitiva	**529**
Hurto por medios informáticos	**2.324**
Transferencia no consentida de activos	**69**

Total: 4.234

Fuente: SPOA

Operaciones transnacionales

FRAUDE EN LINEA

- OPERACIÓN NOSEMA
- OPERACIÓN ACTION DAY FRAUD

MALWARE BANCARIO

- DYRE
- CARBANAK
- TIMBA
- DRYDEX
- CORKOW

DARKNET

- ONYMOUS
- DARKODE
- IOS VI

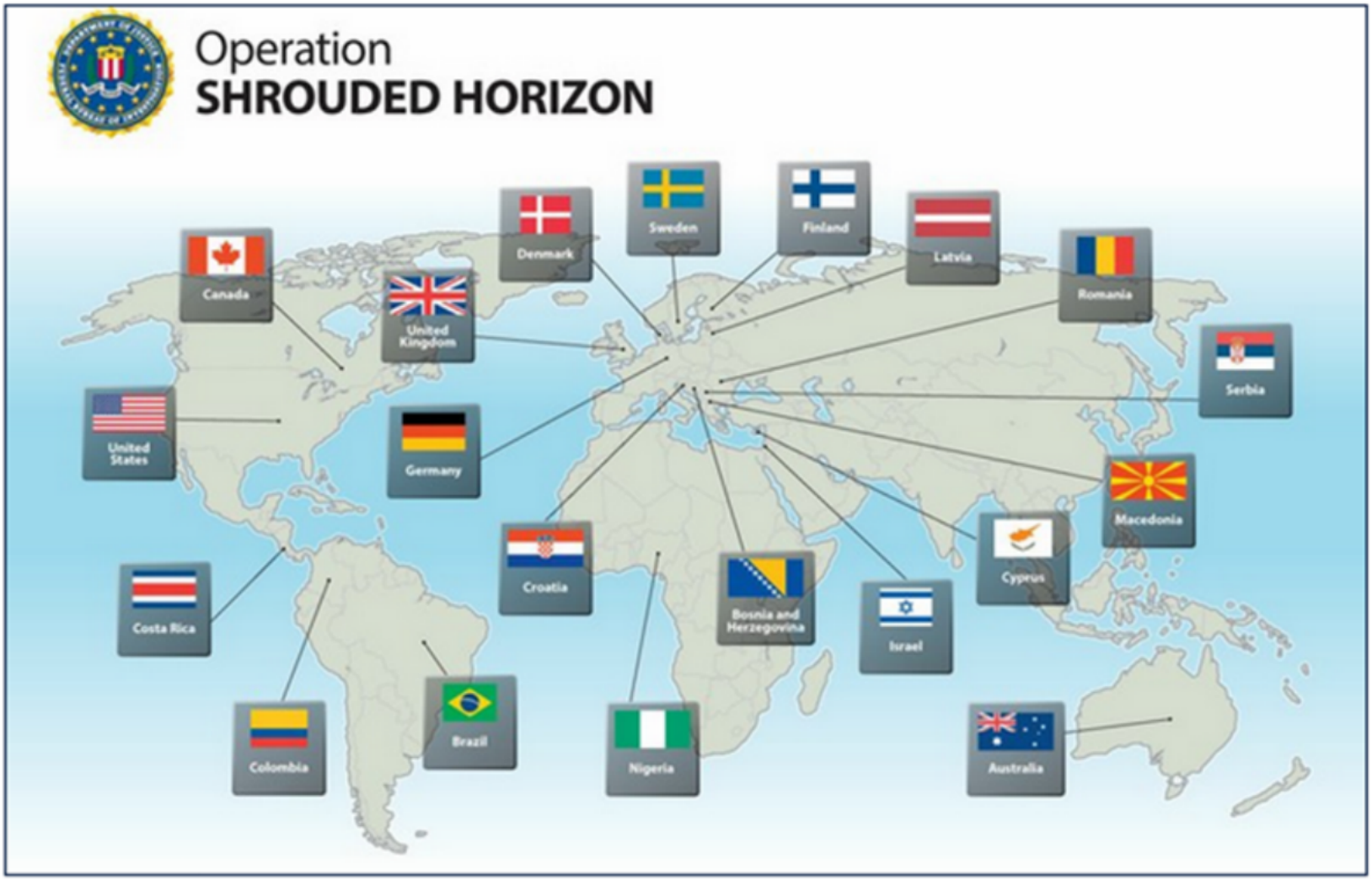
PORNOGRAFÍA INFANTIL

- DEPLATION WAVE 3
- OPERACIÓN PACIFIER
- DEPLETION LATVIA
- OPERATION MOULIN ROUGE
- SIN FRONTERAS

HACKTIVISMO

- UNMASK


NCA
National Crime Agency
AFP
AUSTRALIAN FEDERAL POLICE
POLITI
Polisen
Swedish Police
Bundeskriminalamt
WELCOME TO DARKODE
"International marketplace for sewing machines and other legal stuff"
Profile • Private Messages • Search • FAQ • Memberlist • Usergroups • Log out
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
DEPARTMENT OF JUSTICE
QUI PRO DOMINA JUSTITIA SEQUITUR
EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL
This domain and website have been seized by the Federal Bureau of Investigation, Pittsburgh Field Office and the United States Attorney's Office for the Western District of Pennsylvania as part of a joint law enforcement operation by the F.B.I. and international law enforcement agencies acting through Europol.
POLICIA FEDERAL
ПОЛИЦИЈА
EFCC
ПОЛИЦИЈА
POLICE
CYBER
POLICIJA
DIJIN



The Shrouded Horizon investigation against the Darkode cyber criminal forum involved law enforcement agencies in 20 countries.

Cyber Criminal Forum Taken Down

Members Arrested in 20 Countries

Casos operativos CCP

EL TIEMPO Martes 30 de junio de 2015 | BUSCAR | INGRESA

OPINIÓN COLOMBIA BOGOTÁ MUNDO POLÍTICA ECONOMÍA DEPORTES ENTRETENIMIENTO TECNÓSFERA VIDA

POLÍTICA JUSTICIA PROCESO DE PAZ GOBIERNO CONGRESO PARTIDOS POLÍTICOS

TEMAS DEL DÍA | Farc | Elecciones 2015 | Juan Carlos Pinzón | Corte Constitucional

El ciberdelincuente que viajó por el mundo con millas de los famosos

Robó a sus víctimas creando correos y portales web falsos. Juanes y Sofía Vergara, entre víctimas.

EL TIEMPO Martes 30 de junio de 2015 | BUSCAR | INGRESA

OPINIÓN COLOMBIA BOGOTÁ MUNDO POLÍTICA ECONOMÍA DEPORTES ENTRETENIMIENTO TECNÓSFERA VID

POLÍTICA JUSTICIA PROCESO DE PAZ GOBIERNO CONGRESO PARTIDOS POLÍTICOS

TEMAS DEL DÍA | Farc | Elecciones 2015 | Juan Carlos Pinzón | Corte Constitucional

Así planearon los hackers el robo de $ 160.000 millones

A través de cuentas de ahorro, falsas donaciones y bonos transfirieron millonarias sumas de dinero.

Por: JUSTICIA |

10:35 a.m. | 18 de diciembre de 2014

Semana

El hombre que habría amenazado a Aída Avella y Piedad Córdoba

Semana NACIÓN OPINIÓN ECONOMÍA VIDA MODERNA GENTE CULTURA MUNDO TECNOLOGÍA EDUC

NACIÓN | 2015/06/26 07:50

¿Cómo internet cambió el negocio de las drogas?

Semana NACIÓN OPINIÓN ECONOMÍA VIDA MODERNA GENTE CULTURA MUNDO TECNOLOGÍA EDUC

NOVEDADES | 2014/06/19 00:00

El lado oscuro de internet, refugio para pedófilos

Miles de pedófilos utilizan cada vez más el llamado "lado oscuro de internet" para intercambiar imágenes obscenas de niños, según reveló una investigación de la BBC.

EL TIEMPO Martes 30 de junio de 2015 | BUSCAR | INGRESA

OPINIÓN COLOMBIA BOGOTÁ MUNDO POLÍTICA ECONOMÍA DEPORTES ENTRETENIMIENTO TECNÓSFERA VIDA

ARCHIVO

TEMAS DEL DÍA | Medio ambiente | Elecciones 2015 | Proceso de paz | Violencia contra las mujeres

Roban 500 millones de cuentas bancarias de 29 generales colombianos

La Policía capturó a seis personas responsables del desfalco a las cuentas de los oficiales.

Por: REDACCIÓN JUSTICIA

27 de agosto de 2012

EL TIEMPO Martes 30 de junio de 2015 | BUSCAR | INGRESA

OPINIÓN COLOMBIA BOGOTÁ MUNDO POLÍTICA ECONOMÍA DEPORTES ENTRETENIMIENTO TECNÓSFERA VID

POLÍTICA JUSTICIA PROCESO DE PAZ GOBIERNO CONGRESO PARTIDOS POLÍTICOS

TEMAS DEL DÍA | Farc | Elecciones 2015 | Juan Carlos Pinzón | Corte Constitucional

'Hacker' que atacó 170 páginas web oficiales tiene 17 años

'R4lph_is_here' era la firma que dejaba. Para la Policía es el jefe de Colombian Hackers.

casos operativos e

EL TIEMPO Martes 30 de junio de 2015

BUSCAR INGRESA

OPINIÓN COLOMBIA BOGOTÁ MUNDO POLÍTICA ECONOMÍA DEPORTES ENTRETENIMIENTO TECNÓSFERA VIDA

POLÍTICA

JUSTICIA PROCESO DE PAZ GOBIERNO CONGRESO PARTIDOS POLÍTICOS

TEMAS DEL DÍA | Farc Elecciones 2015 Juan Carlos Pinzón Corte Constitucional

El ciberdelincuente que viajó por el mundo con millas de los famosos

Robó a sus víctimas creando correos y portales web falsos. Juanes y Sofía Vergara, entre víctimas.

Prezi

Semana NACIÓN OPINIÓN ECONOMÍA VIDA MODERNA GENTE CULTURA MUNDO TECNOLOGÍA EDUC

NOVEDADES | 2014/06/19 00:00

El lado oscuro de internet, refugio para pedófilos

Miles de pedófilos utilizan cada vez más el llamado "lado oscuro de internet" para intercambiar imágenes obscenas de niños, según reveló una investigación de la BBC.

Miles de pedófilos utilizan cada vez más el llamado "lado oscuro de internet" para intercambiar imágenes obscenas de niños, según reveló una investigación de la BBC.

Roban 500 millones de cuentas bancarias de 29 generales colombianos

La Policía capturó a seis personas responsables del desfalco a las cuentas de los oficiales.

Por: REDACCIÓN JUSTICIA

27 de agosto de 2012

EL TIEMPO Martes 30 de junio de 2015

BUSCAR INGRESA

OPINIÓN COLOMBIA BOGOTÁ MUNDO POLÍTICA ECONOMÍA DEPORTES ENTRETENIMIENTO TECNÓSFERA VID

POLÍTICA

JUSTICIA PROCESO DE PAZ GOBIERNO CONGRESO PARTIDOS POLÍTICOS

TEMAS DEL DÍA | Farc Elecciones 2015 Juan Carlos Pinzón Corte Constitucional

'Hacker' que atacó 170 páginas web oficiales tiene 17 años

'R4lph_is_here' era la firma que dejaba. Para la Policía es el jefe de Colombian Hackers.

rro, falsas donaciones y bonos transfirieron millonarias sumas de dinero.

Semana | NACIÓN | OPINIÓN | ECONOMÍA | VIDA MODERNA | GENTE | CULTURA | MUNDO | TECNOLOGÍA | EDUC

NACIÓN | 2015/06/26 07:50

¿Cómo internet cambió el negocio de las drogas?


EL TIEMPO
Martes 30 de junio de 2015
BUSCAR
INGRESA
OPINIÓN COLOMBIA BOGOTÁ MUNDO POLÍTICA ECONOMÍA DEPORTES ENTRETENIMIENTO TECNÓSFERA
POLÍTICA
JUSTICIA PROCESO DE PAZ GOBIERNO CONGRESO PARTIDOS POLÍTICOS
TEMAS DEL DÍA
Farc
Elecciones 2015
Juan Carlos Pinzón
Corte Constitucional
Así planearon los hackers el robo de $ 160.000 millones
A través de cuentas de ahorro, falsas donaciones y bonos transfirieron millonarias sumas de dinero.
Por: JUSTICIA |
10:35 a.m. | 18 de diciembre de 2014


Semana
NACIÓN OPINIÓN ECONOMÍA VIDA MODERNA GENTE CULTURA MUNDO TECNOLOGÍA
NACIÓN | 2015/06/26 07:50
¿Cómo internet cambió el negocio

Boletines

CENTRO CIBERNÉTICO POLICIAL

B@CIP - 004 | Boletín de Análisis en CIBERSEGURIDAD PyME

Guía para evitar la suplantación de CLIENTES Y PROVEEDORES

La suplantación es el resultado de la fuga de información en una entidad y el aprovechamiento de una vulnerabilidad existente en un sistema informático. De esta manera, la suplantación de identidad, es aquella técnica empleada por los delincuentes para acceder a pagos, productos o servicios de una entidad.

En este sentido, uno de los aspectos en ciberseguridad que más afecta a las empresas son las estafas al momento de realizar actividades comerciales con clientes y proveedores.

Por tal motivo, en esta guía se brindan algunas recomendaciones básicas para evitar la suplantación de identidad.

¡Inscríbase!

Dirigido a Gerentes Generales, Representantes Legales, Cargos Directivos de Seguridad y Operaciones a nivel mundial, regional y nacional.

Teléfono: 4266200 ext 104010 -104150
Celular: 314442672
Avantel: 123*155
Email: dijin.adepe-fse@policia.gov.co

Fuente del evento: http://www.fse.gov.co/

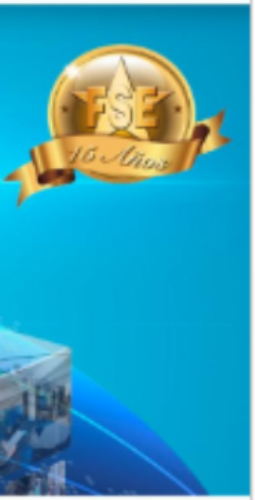
Tendencia
EXTOR

La inclusión pro
conoce como mo
usa tecnología pe
rando así sin la re
toridad central o
brimiento en la t
así como la facili
extorsiones y otro
darknet (red oscu

Ante este panora
nos ciberdelincue
negación distrib
exorsionando así
lantan la mayor p
cial a través de si

01 de sept. de 2015

n de Análisis en
DAD PyME



Generales, Repre-
gos Directivos de
nes a nivel mun-
l.

104010 -104150

@policia.gov.co

//www.fse.gov.co/

1

CENTRO CIBERNÉTICO POLICIAL

B@CIP – 002 | Boletín de Análisis en
CIBERSEGURIDAD PyME

Tendencia de afectación
EXTORSIÓN DDoS

La inclusión progresiva de lo que hoy se conoce como moneda virtual o bitcoin, la cual usa tecnología peer to peer o entre pares operando así sin la regulación legal de alguna autoridad central o banco; ha permitido el encubrimiento en la trazabilidad del cibercrimen, así como la facilidad de pagos instantáneos a extorsiones y otros delitos cometidos desde la darknet (red oscura).

Ante este panorama, desde el año 2014 algunos ciberdelincuentes operan mediante la denegación distribuida de servicios (DDoS), exorsionando así a organizaciones que adelantan la mayor parte de su actividad comercial a través de sitios Web.

Alcance Internacional

Al respecto, el European Cybercrime Centre de EUROPOL alerta sobre el grupo de hackers llamado DD4BC, quienes extorsionan a sus víctimas (empresas) a cambio de no bloquear sus servicios Web. En este sentido, la Organización de los Estados Américanos pone a disposición en su portal Web, la guia IRM #4 que trata sobre la "Respuesta a Incidentes de DDoS".

Ref.: https://www.sites.oas.org

Afectación al
EMAIL SP

Durante estos dos últi
y medianas empresas
por los ataques de ci
municaciones estable
res o clientes, donde
el correo electrónico
nes comerciales.

Este tipo de ataque
spoofing, que consiste
víctima, al hacerle cr
correo electrónico pr
o cliente, cuando en r
la computadora del ci

CENTRO CIBERNÉ

17 de julio de 2015

etín de Análisis en
RIDAD PyME

ional

uropean Cybercrime
, alerta sobre el grupo
DD4BC, quienes ex-
ictimas (empresas) a
ear sus servicios Web.
Organización de los Es-
one a disposición en
uía IRM #4 que trata
sta a Incidentes de

tes.oas.org

CENTRO CIBERNÉTICO POLICIAL

B@CIP - 001 | Boletín de Análisis en
CIBERSEGURIDAD PyME

Afectación al sector PyME
EMAIL SPOOFING

Durante estos dos últimos años, las pequeñas y medianas empresas se han visto afectadas por los ataques de ciberinfiltración a las comunicaciones establecidas con sus proveedores o clientes, donde se emplea como medio el correo electrónico para acordar transacciones comerciales.

Este tipo de ataque se conoce como email spoofing, que consiste en inducir en error a la víctima, al hacerle creer que el mensaje de correo electrónico proviene de un proveedor o cliente, cuando en realidad, es originado en la computadora del ciberdelincuente.

Alcance Internacional

El éxito de los ataques de email spoofing se deriva de la ingeniería social practicada al contexto social de la víctima. Por esta razón, es importante establecer en la empresa un protocolo de atención a eventos de esta índole. Por lo anterior, la Organización de los Estados Américanos pone a disposición en su portal Web la guía IRM #10 que trata sobre "Cómo manejar un incidente de ingeniería social".

Ref.https://www.sites.oas.org

Ataques a cajer
UTILIZANDO EX

El Centro Cibernético Poli
guiente modalidad de ata
debido a que las autoridad
do acerca de una investig
chosos rque tienen relació
utilizando explosivos (TNT

EL 05 de julio de 2015 entr
pechosos, utilizaron masca
senbank" en Austria. Los
spray negro en la cámara
violentaron la bodega de c
ca y colocando el explosi
De este modo, se logró es
tes instalaron 4 tubos de vi
de TNT y un dispositivo elé

15 de julio de 2015

letín de Análisis en
URIDAD PyME

acional

aques de email spoofing
geniería social practicada
l de la víctima. Por esta
nte establecer en la em-
lo de atención a eventos
or lo anterior, la Organi-
dos Américanos pone a
portal Web la guía IRM
re "Cómo manejar un in-
ería social".

ites.oas.org

CENTRO CIBERNÉTICO POLICIAL

B@CIF - 004 | Boletín de análisis en
CIBERSEGURIDAD FINANCIERA

Ataques a cajeros automáticos UTILIZANDO EXPLOSIVOS (TNT)

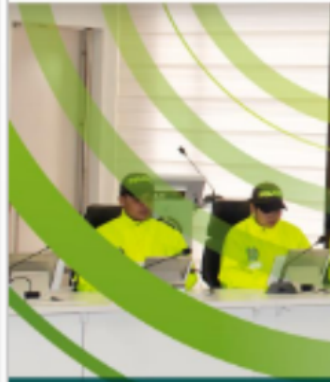
El Centro Cibernético Policial hace difusión de la siguiente modalidad de ataque a cajeros automáticos debido a que las autoridades de Austria han informado acerca de una investigación en contra de sospechosos rque tienen relación con el ataque a un cajero utilizando explosivos (TNT).

EL 05 de julio de 2015 entre las 2:43 y 2:48 horas, sospechosos, utilizaron mascaras e ingresaron al "Raiffeisenbank" en Austria. Los delincuentes emplearon spray negro en la cámara del cajero. Posteriormente, violentaron la bodega de dinero utilizando una palanca y colocando el explosivo en el interior del cajero. De este modo, se logró establecer que los delincuentes instalaron 4 tubos de vidrio rellenos con 10 gramos de TNT y un dispositivo eléctrico.

EUROPOL Enlace internacional

Se emite el presente boletín, en atención al acuerdo de cooperación entre Colombia y la Oficina Europea de Policías EUROPOL, y en concordancia a los compromisos adquiridos con el sector bancario de la Nación en emitir alertas sobre amenazas de ciberseguridad que comprometan la integirdad, disponibilidad y confidencialidad de las trasferencias en cajeros electrónicos y de las entidades bancarias que se vean expuestas a estas amenazas.

CENTRO CIBER
POLIC



Primer portal
www.ccp.

El Centro Cibernético Po
cia de la Dirección de In
INTERPOL, responsable
zos institucionales para
del cibercrimen y ciber
bia.

A partir de la publicació
2011, la Policía Nacional
misional en el marco d
una estrategia nacional
Ciberdefensa, mediante
capacidades para preve
zar y perseguir los incide
berseguridad nacional.

12 de agosto de 2015

Boletín de análisis en
IDAD FINANCIERA

nlace
al

ente boletín, en atención al
eración entre Colombia y la
de Policías EUROPOL, y en
os compromisos adquiridos
cario de la Nación en emitir
nazas de ciberseguridad que
integirdad, disponibilidad y
de las trasferencias en cajeros
las entidades bancarias que
s a estas amenazas.

1

POLICÍA NACIONAL – Dirección de Investigación Criminal e INTERPOL 16 de junio de 2015

CENTRO CIBERNÉTICO POLICIAL

B@CIB – 001 | Boletín de Análisis Estratégico en CIBERSEGURIDAD

Primer portal en ciberseguridad
www.ccp.gov.co

El Centro Cibernético Policial, es la dependencia de la Dirección de Investigación Criminal e INTERPOL, responsable de liderar los esfuerzos institucionales para enfrentar la amenaza del cibercrimen y ciberterrorismo en Colombia.

A partir de la publicación del CONPES 3701 de 2011, la Policía Nacional ha consolidado su rol misional en el marco de la construcción de una estrategia nacional de Ciberseguridad y Ciberdefensa, mediante el desarrollo de las capacidades para prevenir, atender, judicializar y perseguir los incidentes que afectan la ciberseguridad nacional.

Atención en línea 24/7
www.ccp.gov.co

La Ciberseguridad: Es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas, directrices, métodos de gestión del riesgo, acciones de prevención, investigación y atención del delito, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos informáticos y los usuarios en el ciberespacio.

Ref. Directiva Ministerial 2014-18

CENTRO CIBERNÉTICO POLICIAL

B@CIF - 003 | Boletín de Análisis en CIBERSEGURIDAD FINANCIERA

Ataques a cajeros automáticos
ATM ATTACKS

El Centro Cibernético Policial hace difusión de la siguientes modalidades de ataques a cajeros automáticos. Desde el año 2013, estas se han presentado a través del uso de software malicioso y a su vez han aumentado significativamente extendiendose geográficamente causando importantes daños económicos a nivel global.

Sin embargo, no existe un registro centralizado de este tipo de ataques, los cuales en muchos casos, pudieron haberse evitado mediante la aplicación de medidas preventivas.

European ATM Security Team

Es una organización sin ánimos de lucro, cuyo fin principal es la recopilación a nivel europeo de todas las modalidades delincuenciales que atentan contra los cajeros automáticos (ATM), conformando así dos grupos expertos:

1. ATM Fraud (EGAF)
2. ATM Physical Attacks (EGAP)

Ref.: www.european-atm-security.eu

Identity theft
ROBO DE

Los fraudes vinculados
generando cuantiosas pé
ciudadanos del común a
tes suplantan a diario en
acceder ilícitamente a di
tas de crédito ó cuentas
to.

Generalmente los ataque
ginan a partir de episod
documentos por parte d
ción (interna - externa),
de ataques de ingeniería

tín de Análisis en
FINANCIERA

ón sin ánimos de
ncipal es la recopi-
opeo de todas las
incuenciales que
cajeros automáti-
rmando así dos

AF)
tacks (EGAP)

n-atm-security.eu

CENTRO CIBERNÉTICO POLICIAL

B@CIF - 002 | Boletín de Análisis en
CIBERSEGURIDAD FINANCIERA

Identity theft
ROBO DE IDENTIDAD

Los fraudes vinculados a robos de identidad vienen generando cuantiosas pérdidas al sector financiero y a ciudadanos del común a quienes los ciberdelincuentes suplantan a diario en instituciones bancarias para acceder ilícitamente a distintos productos como tarjetas de crédito ó cuentas con cupos de endeudamiento.

Generalmente los ataques de robo de identidad se originan a partir de episodios de pérdida o extravío de documentos por parte de la víctima, fuga de información (interna - externa), o a partir de la combinación de ataques de ingeniería social.

Referencia internacional

Según el IC3 Internet Complaint Center del FBI Federal Bureau of Investigation, en el segundo semestre de 2014, 8.910 personas reportaron incidentes de robo de identidad y las pérdidas ascendieron a U$32.845.753 dólares americanos. Lo que supone el cuarto lugar en cuantía de pérdidas por tipo de crimen según este estudio.

Ver: http://www.ic3.gov/media/annual-report/2014_IC3Report.pdf

CENTRO CIBERNÉ
POLICI

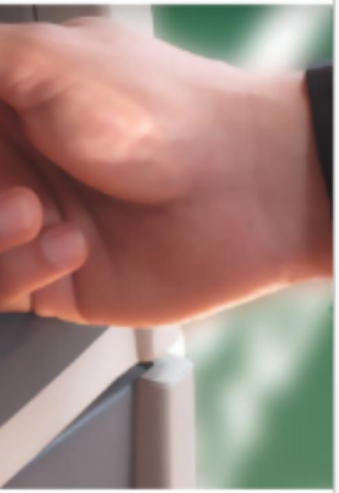
Software malici
DRIDEX

Dridex es un malware tipo
ta el equipo de la víctima
inyección de código HTM
usuarios con identidades
De esta manera, su princi
ner información financie
desde el computador infe

Este código malicioso utili
de botnet, cuando el
equipo trata de comunic
ocultas en deep Web
estas a su vez se comunic
para finalmente reportar
controla toda la red.

01 de junio de 2015

oletín de Análisis en
DAD FINANCIERA



al

ternet Complaint Center del
reau of Investigation, en el
stre de 2014, 8.910 personas
dentes de robo de identidad
ascendieron a U$32.845.753
canos. Lo que supone el
n cuantía de pérdidas por
según este estudio.

ww.ic3.gov/media/annual-
C3Report.pdf

CENTRO CIBERNÉTICO POLICIAL

B@CIF - 001 | Boletín de Análisis en
CIBERSEGURIDAD FINANCIERA

Software malicioso bancario DRIDEX

Dridex es un malware tipo troyano, que infecta el equipo de la víctima a través de spam o inyección de código HTML, engañando a los usuarios con identidades falsas de su origen. De esta manera, su principal objetivo es obtener información financiera y transaccional desde el computador infectado.

Este código malicioso utiliza una arquitectura de botnet, cuando el malware infecta un equipo trata de comunicarse con estaciones ocultas en deep Web llamadas "nodos" y estas a su vez se comunican con varios proxy para finalmente reportarse ante el C&C que controla toda la red.

Enlace internacional

El Centro Cibernético Policial a través de su oficial de enlace en EUROPOL ha recibido información sobre código malicioso originado en Sydney - Australia, cuya modalidad delincuencial es el acceso no atorizado a cuentas bancarias y la transferencia no consentida de dinero. Esta amenaza persiste desde el 15 de julio de 2014 hasta mediados de enero de 2015, afectando el sistema financiero de compañías en 20 países a nivel mundial.

CENTRO CIBERN
POLIC

Fraude con tarj
SKIMMING

El Centro Cibernético Polic
guientes modalidades de a
cos debido a que desde el a
sentado a través del uso de
blecimientos comerciales;
significativamente y se ha
mente causando important

Sin embargo, no existe un
este tipo de ataques, los cu
dieron haberse evitado me
didas preventivas.

15 de mayo de 2015

Boletín de Análisis en
AD FINANCIERA

al

ernético Policial a través
de enlace en EUROPOL ha
rmación sobre código ma-
ado en Sydney - Australia,
dad delincuencial es el
orizado a cuentas banca-
ferencia no consentida de
menaza persiste desde el
2014 hasta mediados de
5, afectando el sistema fi-
compañías en 20 países a

POLICÍA NACIONAL - Dirección de Investigación Criminal e INTERPOL 09 de sept. de 2015

CENTRO CIBERNÉTICO POLICIAL

B@CIF - 005 | Boletín de análisis en
CIBERSEGURIDAD FINANCIERA

Fraude con tarjetas débito y crédito
SKIMMING

El Centro Cibernético Policial hace difusión de las siguientes modalidades de ataques a cajeros automáticos debido a que desde el año 2013, estos se han presentado a través del uso de Skimming en ATMs y establecimientos comerciales; además han aumentado significativamente y se han extendido geográficamente causando importantes daños económicos.

Sin embargo, no existe un registro centralizado de este tipo de ataques, los cuales en muchos casos, pudieron haberse evitado mediante la aplicación de medidas preventivas.

EUROPOL enlace internacional

Se emite el presente boletín, en atención al acuerdo de cooperación entre Colombia y la Oficina Europea de Policías EUROPOL, y en concordancia a los compromisos adquiridos con el sector bancario de la Nación en emitir alertas sobre amenazas que comprometan la ciberseguridad de las transferencias electrónicas de las entidades en distintas plataformas tecnológicas.

European ATM Security Team (EAST)

POLICÍA

CENTRO CIBERNÉ
POLICI

TROYANO F

En lo transcurrido de los ú
han presentado dos ciber
propagado de manera
diante correo electrónico,
suplanta a la Fiscalía Ge
constituyendose así en un
SHING, engañando a las
accedan a un enlace frauc

De esta manera, al ingres
gación se redirige a un ser
el atacante donde se desc
tomáticamente. En esta
colombiano, seguidament
gentino fueron utlizados p

CENTRO CIBERNÉTICO POLICIAL

B@CIB - 003 | Boletín de Análisis en CIBERSEGURIDAD

TROYANO FISCALÍA

En lo transcurrido de los últimos dos meses se han presentado dos ciberamenzas que se han propagado de manera indiscriminada mediante correo electrónico, a través del cual se suplanta a la Fiscalía General de la Nación constituyendose así en una modalidad de PHISHING, engañando a las víctimas para que accedan a un enlace fraudulento.

De esta manera, al ingresar al enlace la navegación se redirige a un servidor vulnerado por el atacante donde se descarga un troyano automáticamente. En esta ocasión un dominio colombiano, seguidamente de un dominio argentino fueron utlizados para este fin.

Alcance Internacional

Al respecto, la Organización de los Estados Américanos pone a disposición en su portal Web, diferentes guías o modelos para la atención de incidentes informaticos. En estos documentos se explica como detectar el incidente, limitar el impacto del ataque, remover la amenaza y recobrar el estado de los sistemas a una etapa normal, así como delinear y mejorar los procesos afectados.

Ref.: https://www.sites.oas.org

| Boletín de análisis en
RIDAD FINANCIERA

enlace
onal

esente boletín, en atención al
operación entre Colombia y la
ea de Policías EUROPOL, y en
a los compromisos adquiridos
bancario de la Nación en emitir
menazas que comprometan la
de las transferencias electróni-
dades en distintas plataformas

Security Team (EAST)

www.ccp.gov.co

@caivirtual

caivirtual

GRACIAS

www.ccp.gov.co

Avenida el Dorado N° 75 25
Teléfono: 426 63 02

FORO INTERNACIONAL SOBRE DELITOS FINANCIEROS

Teniente Coronel FREDY BAUTISTA GARCÍA
Jefe Centro Cibernético Policial