INTERPOL

GLOBAL COMPLEX FOR INNOVATION

Infosecurity México

Adrián ACOSTA

Facilidad de uso criminal

Tecnologías Emergentes - Amplia propagación y enorme impacto

Restricción en el Intercambio de Información

Armonización de Legislación


Experiencia real
el HORMIGUERO 3.0
Sercotel
KRUPS

OTROS DESAFIOS

Afectación a los sistemas computacionales de instituciones financiera

BBC Mundo

NEWS | MUNDO

Noticias América Latina Internacional Economía Tecnología Ciencia Salud Cultura Deportes Video Hay Festival

PUBLICIDAD

Google ha cerrado el anuncio

Dejar de ver anuncio ¿Por qué este anuncio?

México: el ciberataque "sin precedentes" a los bancos del país que causó pérdidas millonarias

Redacción
BBC Mundo

13 mayo 2019

Compartir

Cilianco

5.85
6.50
18.10
19.79
23.20
24.18

Principales noticias

Cómo enseñan la historia de la conquista española en las escuelas de México

Durante varias décadas los mexicanos aprendieron en las aulas que hace 500 años el país fue brutalmente conquistado por los españoles. La versión empieza a cambiar en los programas de estudios, pero en muchos persevera la idea original.

31 marzo 2019

La disculpa del programa Fox & Friends por llamar "3 países mexicanos" a El Salvador, Guatemala y Honduras

31 marzo 2019

"Mamá leona", la madre que mató a uno de los violadores de su hija y que fue perdonada por la justicia

31 marzo 2019

PUBLICIDAD

"Sí, se trata de un ciberataque".

Con estas palabras reconoció el gobernador del Banco de México, Alejandro Díaz de León, que el sistema de transferencias electrónicas de los bancos mexicanos fueron objeto de un hackeo.

La intrusión afectó el **Sistema de Pagos Electrónicos Interbancarios (SPEI)** mediante el cual se procesan cientos de miles de transferencias de dinero entre bancos todos los días.

Se trató de una operación llevada a cabo con rapidez y precisión a finales de abril, cuando varios de los mayores bancos de México detectaron transferencias no autorizadas.

- **Cómo operaban los hackers acusados de hacer que los cajeros automáticos escupieran dinero**

"Este claramente ha sido un ataque que ha impactado a diversos pa
la cadena de pagos electrónicos, que es un ataque de importancia y
menos en el sistema de pagos, **no teníamos antecedentes**", dijo D
lunes.

Aunque el monto del dinero sustraído de los bancos no ha sido dete
diversas fuentes de la prensa en México dicen que oscila entre los 4
millones de pesos (entre US$21 y US$42 millones).

CRÓNICA

Cómo fue el hackeo al Banco de Chile

La sustracción de US$ 10 millones fue el punto cúlmine de una sofisticada operación que duró meses y que puede volver a ocurrir en Chile. Empresas de ciberseguridad alertaron, en noviembre pasado, de este tipo de ataques.

INTERPOL

EL ECONOMISTA 30 ANIVERSARIO

AMLO 2018-2024

CIBERSEGURIDAD

México evitó el mayor hackeo al sistema de comunicaciones SWIFT

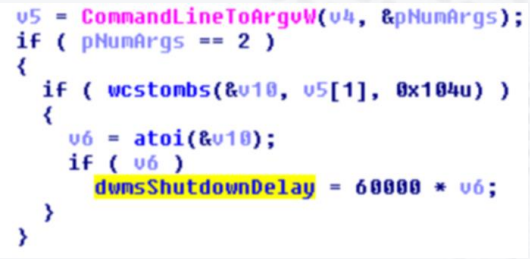
Si, en enero pasado, los atacantes del Banco Nacional de Comercio Exterior (Bancomext) hubieran conseguido su objetivo, este incidente se habría convertido en el mayor robo cometido en contra de una institución financiera a través de un sistema de pagos interbancarios.

Rodrigo Riquelme
11 de junio de 2018, 15:48

HACKEOS A BANCOS A TRAVÉS DE SISTEMAS DE PAGOS INTERBANCARIOS

El hackeo al Banco de Chile se suma a la lista de instituciones financieras afectadas por ataques que aprovecharon vulnerabilidades en sus sistemas de conexión con plataformas de pagos interbancarios nacionales e internacionales.

Malware denominado TROJ_KILLDISK.IUB



Referido ataque fue perpetrado empleando el archivo dimens.exe el cual el día del ataque (9 de enero de 2018) aún era del tipo día 0, es decir no existían incidencias previas de este malware en las bases de firmas de antivirus o soluciones de seguridad.

Este malware denominado TROJ_KILLDISK.IUB, fue alojado el día 09 de enero de 2018 fecha del ataque, en 456 computadoras de un total de 788 (57% afectadas) Pertenecientes a la red bancaria de México, 10 minutos antes de realizar las transacciones ilegítimas, una vez alojado, se ejecuta de manera automática y forzar el reinicio, de esta manera deja inservible el sistema operativo de la máquinas afectadas provocando que la atención principal fuera hacia este incidente pasando en ese momento desapercibidas las transacciones ilegitimas al sistema SWIFT.

INTERPOL

BEC

Businesse Email Compromise

BUSINESS EMAIL COMPROMISED

Comprometiendo el correo electrónico a través de la ingeniería social, el phishing
Uso de malware no sofisticado, por ejemplo, Keylogger

Una red de criminales que concreta el plan

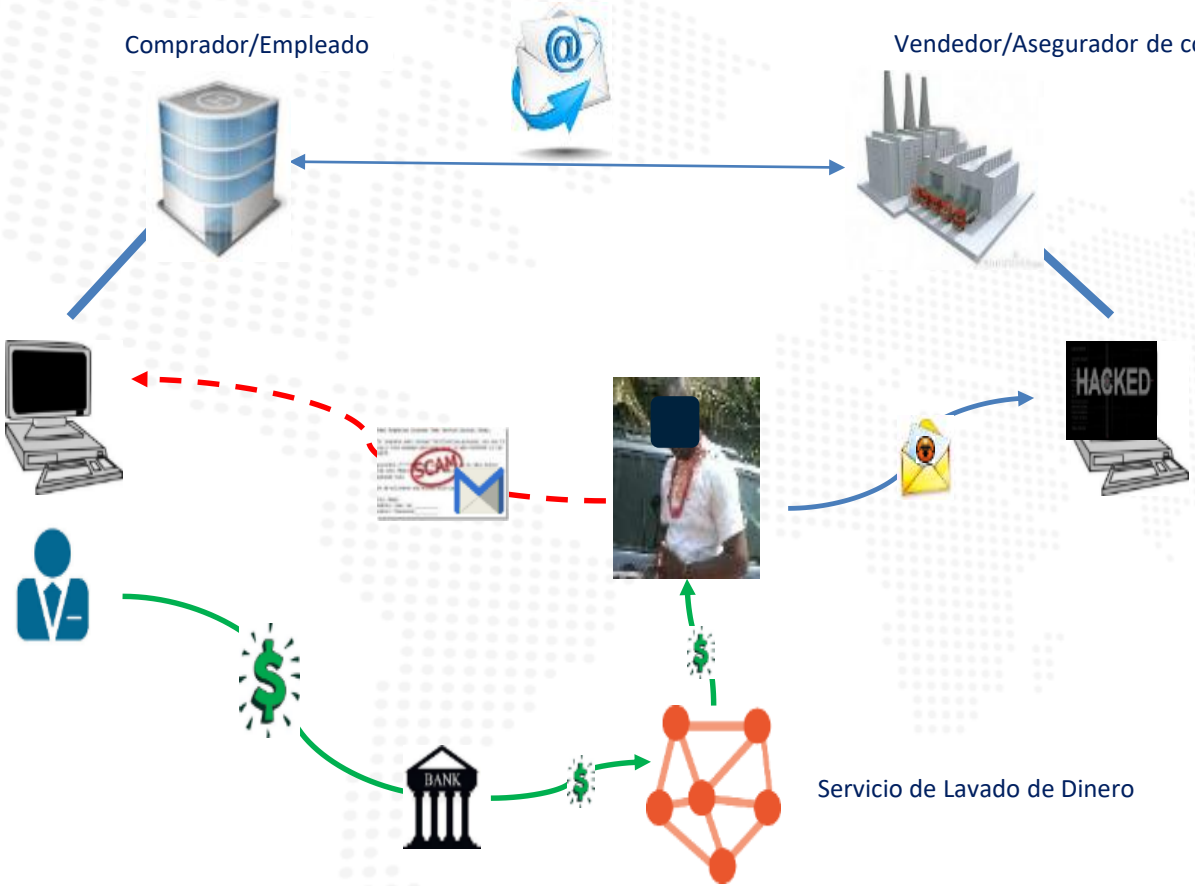
Monitor de intercambio de correo electrónico o toma de cuenta
Comprensión del modelo de negocio, actividades, relaciones, etc.

Enviar correo electrónico para solicitar una transferencia de fondos
A través de una cuenta de correo electrónico comprometida o correo electrónico falso

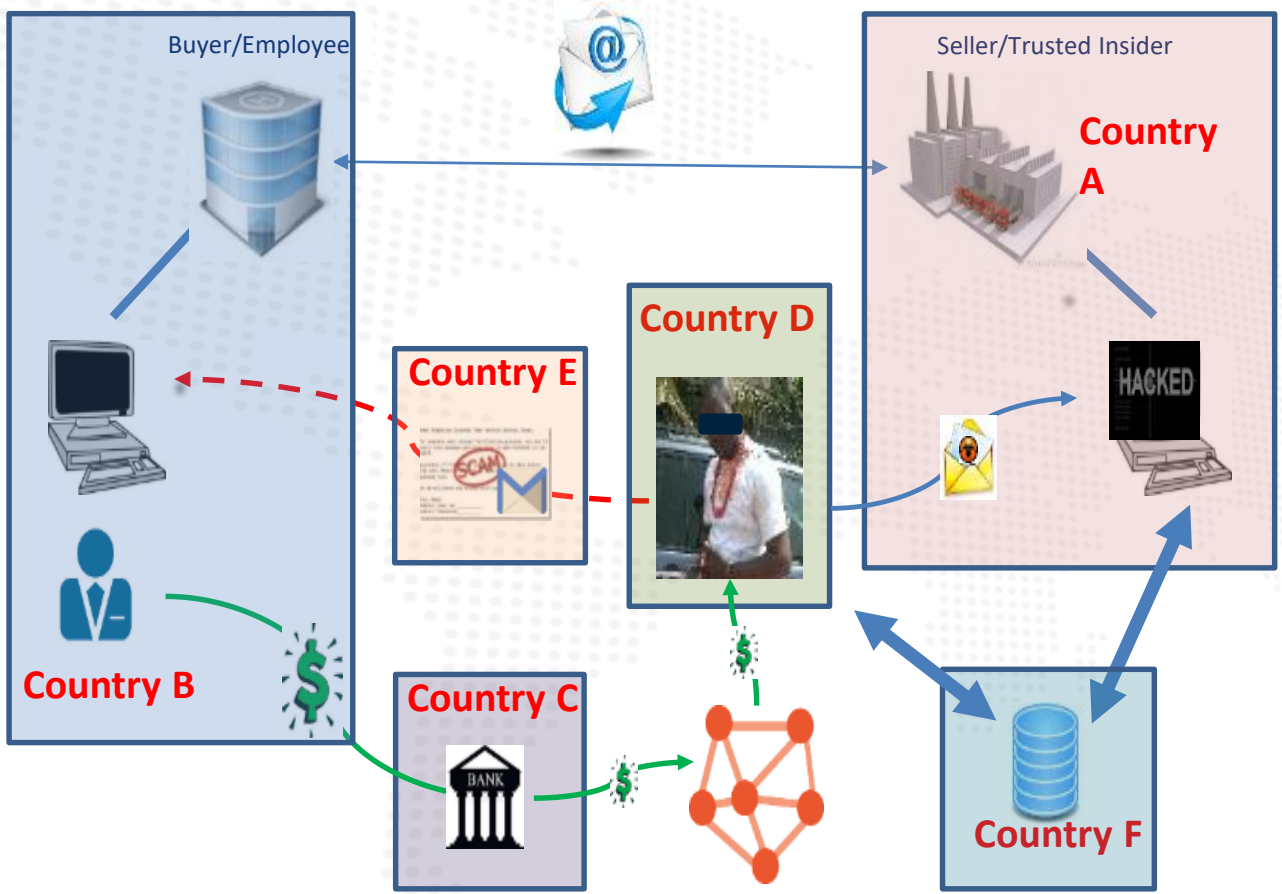
Transferido el pago
A la cuenta designada de Criminal

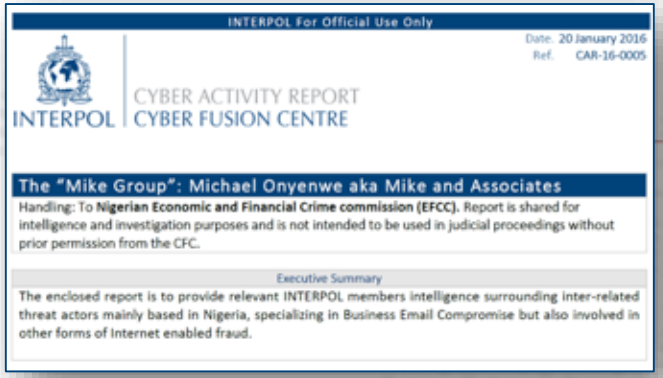
Dinero transferido a través de la red de mulas monetarias

Business E-mail Compromise



Jurisdictional Issues





INTERPOL For Official Use Only

Date: 20 January 2016
Ref. CAR-16-0005

INTERPOL | CYBER ACTIVITY REPORT
CYBER FUSION CENTRE

The "Mike Group": Michael Onyenwe aka Mike and Associates

Handling: To **Nigerian Economic and Financial Crime commission (EFCC).** Report is shared for intelligence and investigation purposes and is not intended to be used in judicial proceedings without prior permission from the CFC.

Executive Summary

The enclosed report is to provide relevant INTERPOL members intelligence surrounding inter-related threat actors mainly based in Nigeria, specializing in Business Email Compromise but also involved in other forms of Internet enabled fraud.

Líder de la red mundial detrás de miles de estafas en línea es arrestado en Nigeria

Se cree que este nigeriano de 40 años de edad, conocido como 'Mike', está detrás de estafas por un total de más de 60 millones de dólares que involucran a cientos de víctimas en todo el mundo. En un caso, un objetivo fue estafado para que pagara 15,4 millones de dólares..

Cargos incluyendo piratería informática, conspiración y obtención de dinero con pretextos falsos.

Business Email Compromised

Los negocios objetivo eran el fraude de desvío de pagos -en el que el correo electrónico de un proveedor se pondría en peligro y se enviarían mensajes falsos al comprador con instrucciones para el pago a una cuenta bancaria bajo el control del delincuente- y el "fraude del director general".

OTROS DESAFIOS

Criptoactivos

Cryptojacking

Malware que generalmente compromete los sitios web públicos para posteriormente obtener el poder de procesamiento de los visitantes del sitio, sin que lo sepan, y utiliza esa potencia para extraer criptomonedas a través de técnicas de minería de datos.

¡Hola!

Puede que no me conozca y probablemente esté preguntándose por qué está recibiendo este correo electrónico, ¿correcto?
En este momento pirateé tu cuenta (comec@adinet.com.uy). ¡Tengo pleno acceso a tu dispositivo! Te envio un correo electrónico desde tu cuenta !
De hecho, coloqué un malware en el sitio web de videos para adultos (material pornográfico) y usted sabe qué, usted visitó este sitio web para divertirse (ya sabe a qué me refiero).
Mientras estabas viendo clips de video,
su navegador de Internet comenzó a funcionar como un RDP (escritorio remoto) que tiene un registrador de teclas que me proporcionó acceso a su pantalla y también a su cámara web.
Inmediatamente después, mi programa de software reunió todos sus contactos desde su Messenger, redes sociales y correo electrónico.

¿Qué hice?
Hice un video de doble pantalla. La primera parte muestra el video que estabas viendo (tienes un buen gusto ya veces extraño), y la segunda parte muestra la grabación de tu cámara web.
¿Exactamente qué deberías hacer?

Bueno, creo que $250 es un precio justo para nuestro pequeño secreto.
Realizará el pago con Bitcoin (si no lo sabe, busque "cómo comprar bitcoin" en Google).
Dirección de BTC: 1LK8rRhBTekN3Uxh8ib83FfmvMsX6EQnqL
(Es muy sensible, así que cópielo y péguelo)

Nota:
Tienes 2 días para hacer el pago.
(Tengo un píxel específico en este mensaje de correo electrónico, y en este momento sé que ha leído este mensaje de correo electrónico).

Si no obtengo los BitCoins, definitivamente enviaré su grabación de video a todos sus contactos, incluidos familiares, compañeros de trabajo, etc.

Sin embargo, si pagas, destruiré el video inmediatamente.
Si desea pruebas, responda con "¡Sí!" y enviaré tu grabación de video a tus 3 amigos
Esta es la oferta no negociable, así que no pierda mi tiempo personal y el suyo respondiendo a este mensaje de correo electrónico.

La próxima vez, ¡ten cuidado!
¡Adiós!

Hola

Puede que no me conozca y probablemente este preguntándose por que esta recibiendo este correo electrónico ¿correcto?
En este momento piratee tu cuenta. tengo pleno acceso a tu dispositivo!
De hecho, coloque un malware en el sitio web de videos para adultos (material pornográfico) y usted sabe que, usted visito este sitio web para divertirse (ya sabe a que me refiero)
Mientras estaba viendo clips de video.
Su navegador de Internet comenzó a funcionar como un RDP (escritorio remoto) que tiene un registrador de teclas que me proporciono acceso a su pantalla y también a su cámara web.
Inmediatamente después, mi programa de software reunión todos sus contactos desde su Messenger, redes sociales y correo electronico

¿Qué hice?
Hice un video de doble pantalla. La primera parte muestra el video que estabas viendo (tienes un buen gusto ya veces extraño), y la segunda parte muestra la grabación de tu cámara web.

¿Exactamente que deberías hacer?
Buen. Creo que $250 es un precio justo para nuestro pequeño secreto.
Realizara el pago con Bitcoin (si no lo sabe, busque “como comprar bitcoin” en Google)
Dirección de BTC 1LK3rTeknewch84FtmvMsXGEnque.
(Es muy sensible, así que cópielo y péguelo)

INTERPOL

Nota:
Tienes 2 días para hacer el pago.
(Tengo un pixel especifico en este mensaje de correo electronico, y en este momento se que ha leído este mensaje de correo electronico)

Si no obtengo los Bitcoins, definitivamente enviare su grabación de video a todos sus contactos, incluidos familiares, compañeros de trabajo, etc.

Sin embargo si pagas, destruiré el video inmediatamente.
Si desea pruebas, responda con “¿SI!” y enviare tu grabación de video a tus 3 amigos.

Esta es la oferta no negociable, asi que no pierda mi tiempo personal y el suyo respondiendo a este mensaje de correo electronico

La próxima vez ten cuidado

Adios..

SI TE LLEGA UN MAIL QUE TIENE COMO ASUNTO:

tu cuenta de correo electrónico @suservidor.com fue pirateada

(Aclarando que tanto el remitente como el destinatario resulta ser el mismo y en cuyo cuerpo del mensaje informan que se ha colocado un MALWARE, en un sitio WEB de videos para adultos y en el que se solicita un pago con moneda virtual "BITCOIN")

¡IGNORALO!

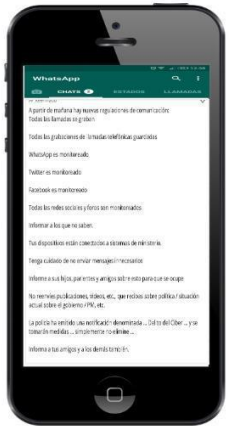
Este tipo de mensajes son una técnica bastante conocida, que apela a la ingeniería social para engañar al destinatario y obligarlo a efectuar un pago en moneda virtual.

¡NO CAIGAS!

PFA POLICÍA SEGURIDAD DE ESTADO

Ministerio de Seguridad
Presidencia de la Nación

Cuidado con los falsos mensajes



OTROS de los mensajes que circulan en cadena es en la Red Social WhatsApp, sobre una supuesto aviso de una nueva regulación de que las llamadas y mensajes estarían siendo grabadas y monitoreadas. **ESTO ES FALSO….**

INSISTIMOS: en no reenviar las noticias o menajes que no estén respaldadas por persona física o jurídica responsable, o en su caso sin haber corroborado la procedencia.

NO TE DEJES MANIPULAR…….Piensa antes de

Ministerio Público
República del Paraguay
Fiscalía con la gente

GOBIERNO NACIONAL

Paraguay de la gente

Cuidado con los falsos mensajes

En los últimos días se han recibido decenas de reportes de usuarios que dicen estar recibiendo correos extorsivos (sextorsión) sobre el supuesto **"pirateo"** de su computadora y la consecuente exposición de archivos privados sensibles, como fotos y videos. El correo habla de la instalación de un RAT (Remoto Access Trojan) que permitiría al delincuente espiar las acciones y archivos del usuario afectado **Por supuesto todo es mentira pero, como se verá, los usuarios pueden dudar de la veracidad del correo e incluso llegar a pagar.**

Bajo ninguna circunstancia se debe responder y mucho menos pagar.

Ministerio Público
República del Paraguay
Fiscalía con la gente

GOBIERNO NACIONAL

Paraguay de la gente

INTERPOL


55% 11:32 p. m.
PDI
.cl
para mí
6:09 p. m.
FALSO
CIBERCRIMEN
¡Hola!
Puede que no me conozca y probablemente esté preguntándose por qué está recibiendo este correo electrónico (@ .cl), ¿correcto?
En este momento pirateé tu cuenta (Dominio). ¡Tengo pleno acceso a tu dispositivo!
De hecho, coloqué un malware en el sitio web de videos para adultos (material pornográfico) y usted sabe qué, usted visitó este sitio web para divertirse (ya sabe a qué me refiero).
Mientras estabas viendo clips de video,
su navegador de Internet comenzó a funcionar como un RDP (escritorio remoto) que tiene un registrador de teclas que me proporcionó acceso a su pantalla y también a su cámara web.
Inmediatamente después, mi programa de software reunió todos sus contactos desde su Messenger, redes sociales y correo electrónico.
¿Qué hice?
Hice un video de doble pantalla. La primera parte muestra el video que estabas viendo (tienes un buen gusto ya veces extraño), y la segunda parte muestra la grabación de tu cámara web.
¿Exactamente qué deberías hacer?
Bueno, creo que $200 es un precio justo para nuestro

INTERPOL

- **CIBER-RESILIENCIA**

Metodología de gestión de riesgo estructurada para enfrentar y mitigar las consecuencias de una crisis de ciberseguridad.

INTERPOL

Jules Verne

Cualquier cosa que un hombre pueda imaginar, otros hombres podrán hacerla realidad.

Criminales

https://en.wikipedia.org/wiki/Jules_Verne

Future Crime

Muchas Gracias

Adrian Eduardo Acosta