Rumbo de la Ciberseguridad en Costa Rica

COSTA RICA
Ministerio Público
... para una Justicia Democrática

Emilia Navas

Diciembre 2016

Indicadores a Nivel Internacional en Ciberseguridad

Objetivos Principales:
- Gobierno.
- Sector Financiero.
- Infraestructura Crítica.
- Privado y Médico.

Actores Ataques:
- Crimen Organizado.
- Grupos Hactivistas.
- Adversarios Comerciales.
- Terrorismo.
- Personas Individuales.

Motivos Atacar:
- Ganancia Económica.
- Espionaje.
- Sabotaje.
- Manifestaciones Virtuales
- Vengansa.

Robo de Información:
- 37 cada segundo.
- 2.237 cada minuto.
- 134.236 cada hora.

Fuente: Breachlevelindex.com (Estadística de Abril 2016)

Nivel Madurez Actual de Costa Rica

Fuente: Informe Ciberseguridad 2016 de la OEA – www.observatoriociberseguridad.com

Nivel Madurez Actual de Costa Rica - Continuación

Tecnologías

Adhesión a las normas
- Aplicación de las normas y prácticas mínimas aceptables
- Adquisiciones
- Desarrollo de softwre

Organizaciones de coordinación de seguridad cibernética
- Centro de mando y control
- Capacidad de respuesta a incidentes

Respuesta a incidentes
- Identificación y designación
- Organización
- Coordinación

Resiliencia de la infraestructura nacional
- Infraestructura tecnológica
- Resiliencia nacional

Protección de la Infraestructura Crítica Nacional (ICN)
- Identificación
- Organización
- Planeación de respuesta
- Coordinación
- Gestión de riesgos

Gestión de crisis
- Planeación
- Evaluación

Redundancia digital
- Planeación
- Organización

Mercado de la ciberseguridad
- Tecnologías de seguridad cibernética
- Seguros de delincuencia cibernética

Educación

Disponibilidad nacional de la educación y formación cibernéticas
- Educación
- Formación

Desarrollo nacional de la educación de seguridad cibernética
- Desarrollo nacional de la educación de seguridad cibernética

Formación e iniciativas educativas públicas y privadas
- Capacitación de empleados en seguridad cibernética

bernanza corporativa, conocimiento y normas
- Comprensión de la seguridad cibernética
- parte de empresas privadas y estatales

Fuente: Informe Ciberseguridad 2016 de la OEA – www.observatoriociberseguridad.com

Situación Actual en Costa Rica

Iniciativas en diferentes sectores:

- MICIIT: CSIRT-CR.
- Iniciativas del Sector Público y Privado: Comisión de Seguridad Bancaria.
- Cooperación Internacional: OEA.
- Convenio Budapest (2001): Asamblea Legislativa.

Se requiere **Convergencia** para que a nivel **país** se mejoren los eslabones débiles de la cadena.

¿Cómo Afrontar los Retos?

Temas **Nacionales** a Intervenir y Solucionar en **4 Ejes** Principales:

Legislación

1. Apego Convenio Budapest (**No** se ha ratificado).
2. Análisis Leyes Nacionales Aplicables:

- Ley Delitos Informáticos.
- Ley de Protección de las Personas frente al tratamiento de sus datos personales.
- Ley de Información no divulgada.

Educación

1. Concientización **Ciudadanía**.
   - Prácticas de Protección.
2. Concientización, Capacitación y Formación **Empleados**.
   - Prácticas de Protección.
   - Prácticas de Prevención.
   - Prácticas de Respuesta.
   - Gestión de Riesgos.

Buenas Prácticas de Seguridad

Sector Público y Privado

1. Aplicación de Normas, Marcos o Estándares:
   - ISO/IEC 27001.
   - NIST.
   - Cobit 5.
   - Arquitecturas de Seguridad.
2. Políticas Específicas Internas:
   - Evaluación Amenazas.
   - Evaluación Vulnerabilidades.
   - Gestión Riesgos.
   - Auditorías.
   - Gestión de Incidentes de Seguridad.

Cooperación Internacional

1. Reconocimiento internacional por parte de entidades que pueden colaborar en la respuesta a incidentes:
   - CERT´s de países.
   - Acuerdos Internacionales de Apoyo como la OEA.
   - Interpol.

Plan de Acción

Integración de los 4 elementos descritos dentro de la **estrategia del país**, para hacer frente a las necesidades de comprensión, protección y aseguramiento de la Ciberseguridad en todos los ámbitos.

Caso de Extorsión, Ataque Cibernético y Suplantación de Identidad

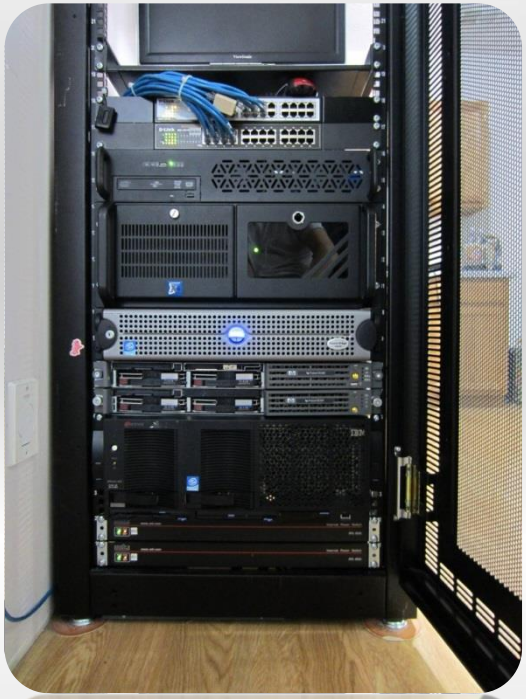
COSTA RICA
Ministerio Público
... para una Justicia Democrática

Fecha del Caso: Marzo 2016

Emilia Navas

Escenario del Caso

Un Proveedor Servicios de Internet (ISP), dentro de su cartera de servicios ofrece la posibilidad de alquilar o rentar espacios en su datacenter (Servicios de Colocación) para que clientes alojen sus servidores, discos duros y sus respectivas aplicaciones asegurando la alta disponibilidad.



Escenario del Caso - Continuación

ISP

- El ISP oficializa el servicio por medio de sus ejecutivos de cuenta, debido a que es un servicio empresarial

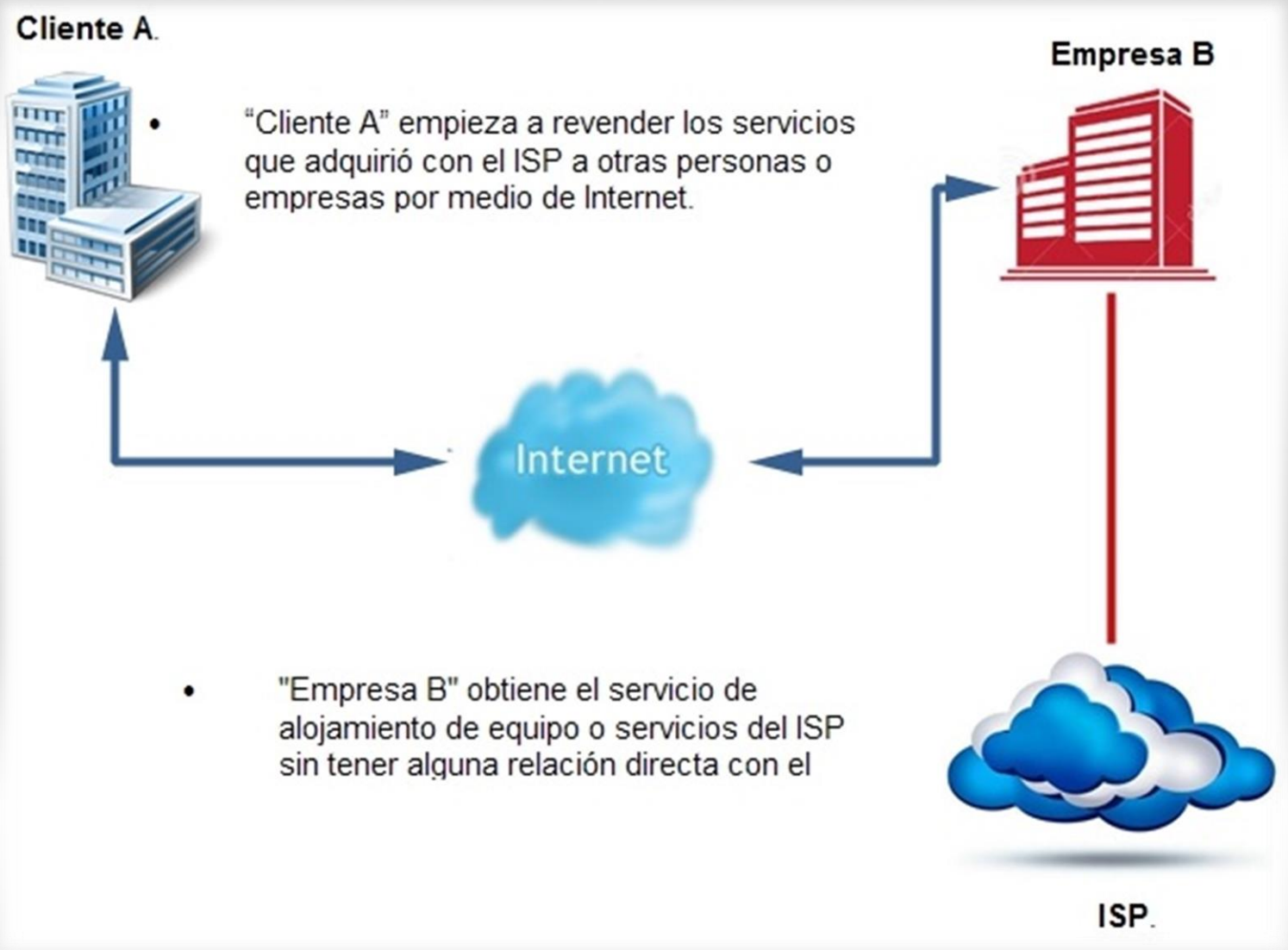
Ejecutivos Ventas

- Los ejecutivos de venta formalizan el servicio por medio de un contrato con los clientes

Cliente A

- "Cliente A" obtiene el servicios y accesos respectivos según estipula en el contrato

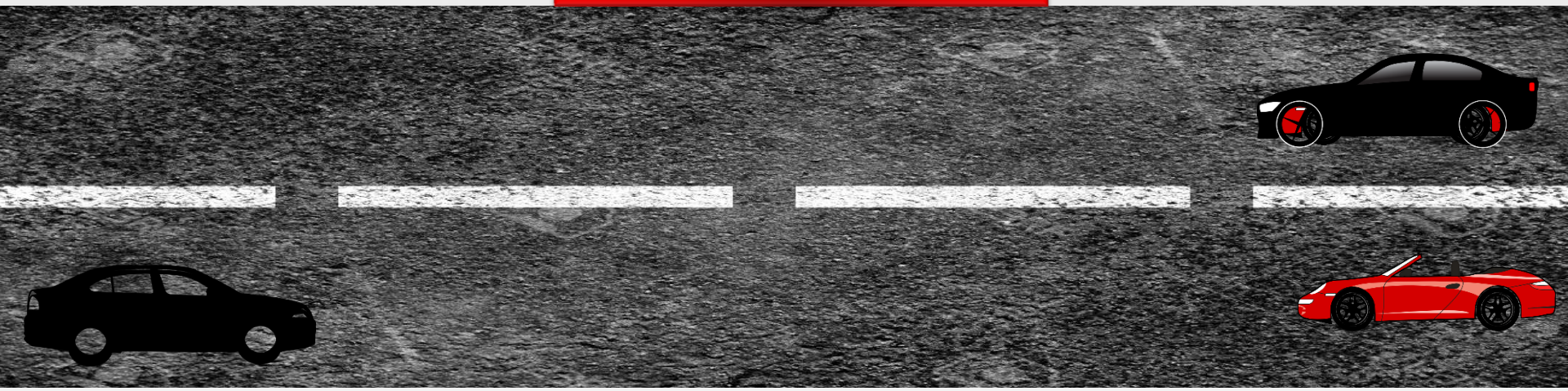
Escenario del Caso - Continuación



Inicio de los Ataques

El ISP empieza a identificar ataques de **Denegación de Servicio Distribuidos (DDoS)** dirigidos hacia el “Cliente A”, por lo que las herramientas de monitoreo disparan las alertas y es tratado como un incidente normal y le notifican al “Cliente A” de la situación.

Saturación o Degradación del Servicio



Denegación de Servicio (Dos - DDoS): es la acción que limita el uso autorizado de redes, sistemas o aplicaciones, al enviar gran cantidad de paquetes (vehículos) a la red (carretera) .

Mensajes de Extorsión

From: sylvain harlin <sylain-harlin34@outlook.fr>
To: "isp@isp.co.cr"
Subject: Attack website DDOS - Warning

hello, you host a french site illegal.
a child pornography website on Tor.
ip site : **190.10.9.188**
I close their website, Attack DDOS, I will continue the attack.

If you are not close the french site, I will focus on you.
Delete the site and no backup restore, I will inform the french general int=
elligence and cybercrime and child protection, for crimes against humanity.

you are warned...I do not demand ransom, just close the french site.

waiting for an answer

Anonymous.

Análisis de los Registros

Datos de la Dirección IP 190.10.9.188:

Cliente: Hensley Anthony Samuel – **Nombre Falso.**

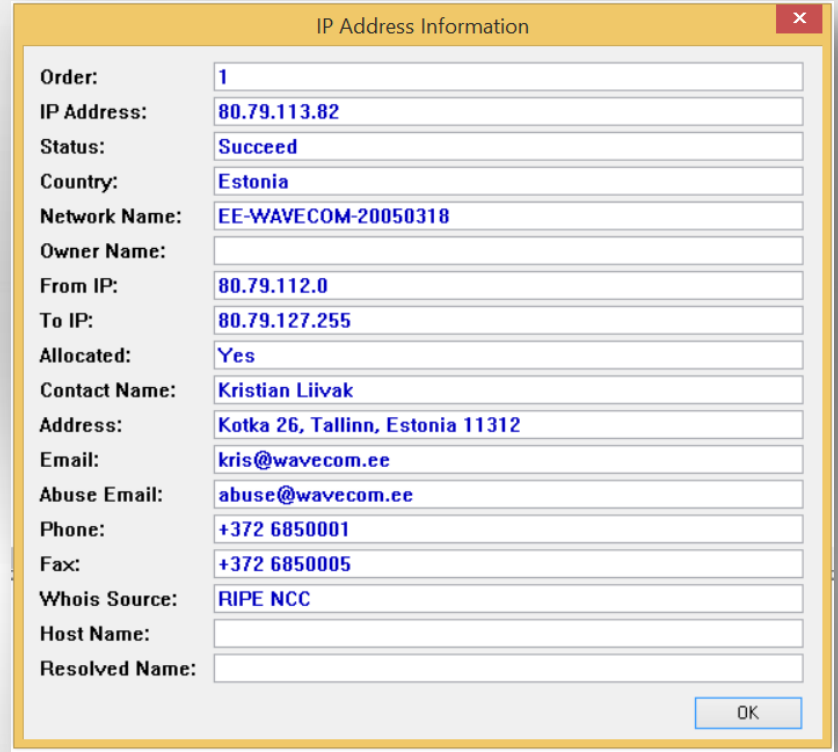
Organización: Private – **No se asoció ninguna empresa**.

Teléfono: 7708895698 – **no corresponde a una numeración en Georgia.**

Email: hensley_anthonysamuel@aol.com.

País: USA, Georgia.

Primera Conexión desde la IP: 80.79.113.82

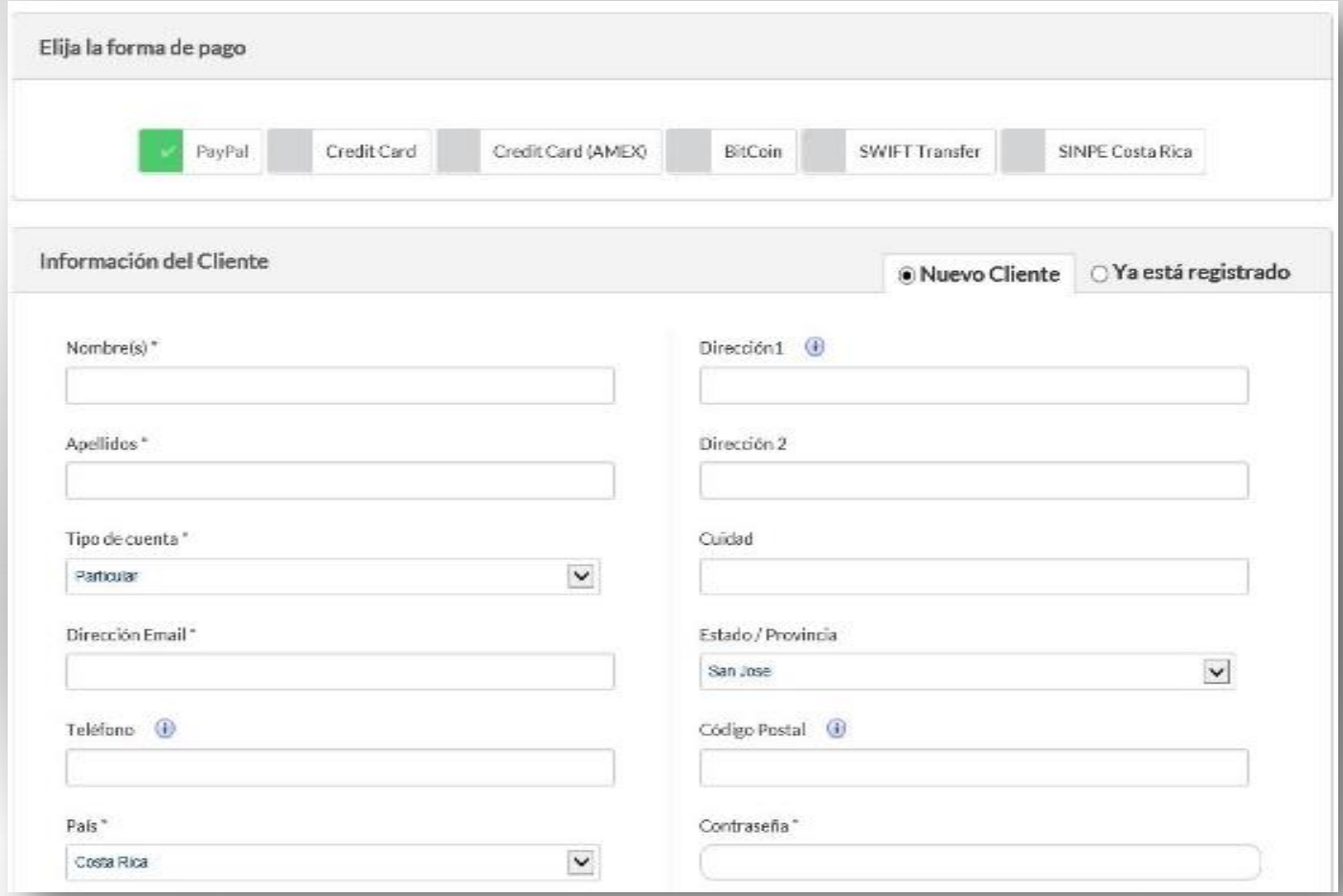


IP Address Information

Order:	1
IP Address:	80.79.113.82
Status:	Succeed
Country:	Estonia
Network Name:	EE-WAVECOM-20050318
Owner Name:	
From IP:	80.79.112.0
To IP:	80.79.127.255
Allocated:	Yes
Contact Name:	Kristian Liivak
Address:	Kotka 26, Tallinn, Estonia 11312
Email:	kris@wavecom.ee
Abuse Email:	abuse@wavecom.ee
Phone:	+372 6850001
Fax:	+372 6850005
Whois Source:	RIPE NCC
Host Name:	
Resolved Name:	

OK

Método de Pago



Supuesta Orden Judicial de la Policía Francesa

PREFECTURE DE POLICE

Direction de la Police judiciare
Brigade de la répréssion de la lutte Anti-terrorisme
Direction générale de la Sécurité intérieure
DGSI

REQUISITION JUDICIAIRE

Dossier : 84492FR
Mandat : 47552016FR

PARIS, le 03 avril 2016

Affaire suivie par : Patrick Calvar **Directeur général de la Sécurité intérieure**

Nous, officier de Police Judiciaire en résidence à PARIS

Poursuivant l'éxécution de la commission rogatoire émanant du cabinet de la DGSI et de la lutte contre le terrorisme sur le territoire Français.
Le Directeur Patrick Calvar référencé en ses services sous le numéro : 47552016FR et délivrée le 03 Avril 2016 par le Tribunal de Grande Instance de Paris dans le cadre d'un hébergement illégal d'un site faisant L'apologie du terrorisme ou l'incitation aux actes de terrorisme sur le Territoire Français et hébergement de contenu pédopornographique.

Et vu les articles 81, 251, 13-2 du Code de Procédure Pénale

Prions et aux besoins à l'effet de bien vouloir nous communiquer :

Tous les éléments en vôtre possession concernant le site qui à été héberger sur vos serveurs
Les infos du directeur de Publication (identité complète : Nom, Prénom, filiation, adresse, téléphone, mail, sauvegarde de fichiers et fichiers hébergé, base de données, etc..)

site connu du nom : Black Hand

L'IP signaler retenu : 190.10.9.188
Nous attendons vos renseignements et vôtre collaboration dans les plus bref délais pour assurer la sécurité du Territoire Français.

Le Capitaine de Police

¡Muchas Gracias!

Emilia Navas
Teléfono: 506-2295-3000
Correo electrónico:
enavas@poder-judicial.go.cr