Modalidades de ataques de ciberseguridad en Latinoamérica

Foco: Sector Marítimo

Diego Subero
Oficial del Programa de Ciberseguridad
Secretaría del Comité Interamericano contra el Terrorismo (CICTE)

The opinions expressed in this presentation do not necessarily reflect the views of the General Secretariat of the Organization of American States or the governments of its member states.

Diego Subero

OAS Cybersecurity Program
Organization of American States

cybersecurity@oas.org

@OEA_Cyber

Agenda

Situación Global

Ciberseguridad en el Sector Marítimo

Cómo atacan

Cyber Kill Chain

Reconocimiento ***(Reconnaissance)***

Militarización ***(Weaponization)***

Entrega ***(Delivery)***

Explotación ***(Explotation)***

Instalación ***(Installation)***

Mando y control ***(Command & control)***

Acciones ***(Actions)***

Ingeniería social

Algunos ataques en crecimiento en la región

Ransomware

Ataques BEC

Formjacking

Nuevas formas de ciberdefensa

Situación Global

Ataques globales

2016

APT 28 Y 29- USA Elecciones

SWIFT
Ataque orientado a sistemas swift banca

Ataque DDOS causa caída en Twitter, Spotify, y otros sitios

2017

Hacking Group - Lazarus
Campaña en 31 Paises

Elecciones Francia
Leaked de correo de Emmanuel Macron

Global Ransomware Attacks
WannaCry y Petya

2018-19

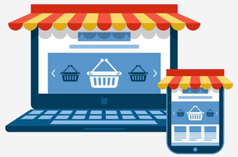
Divulgación de información Facebook's
87 millones de perfiles de usuarios

Cambridge Analytica

Ataque ransomware en Atlanta city
SamSam Ransomware
16 años de data
$ 2.6 millions en recovery

DDOS bases in IoT

Formjacking..
Ataque en crecimiento

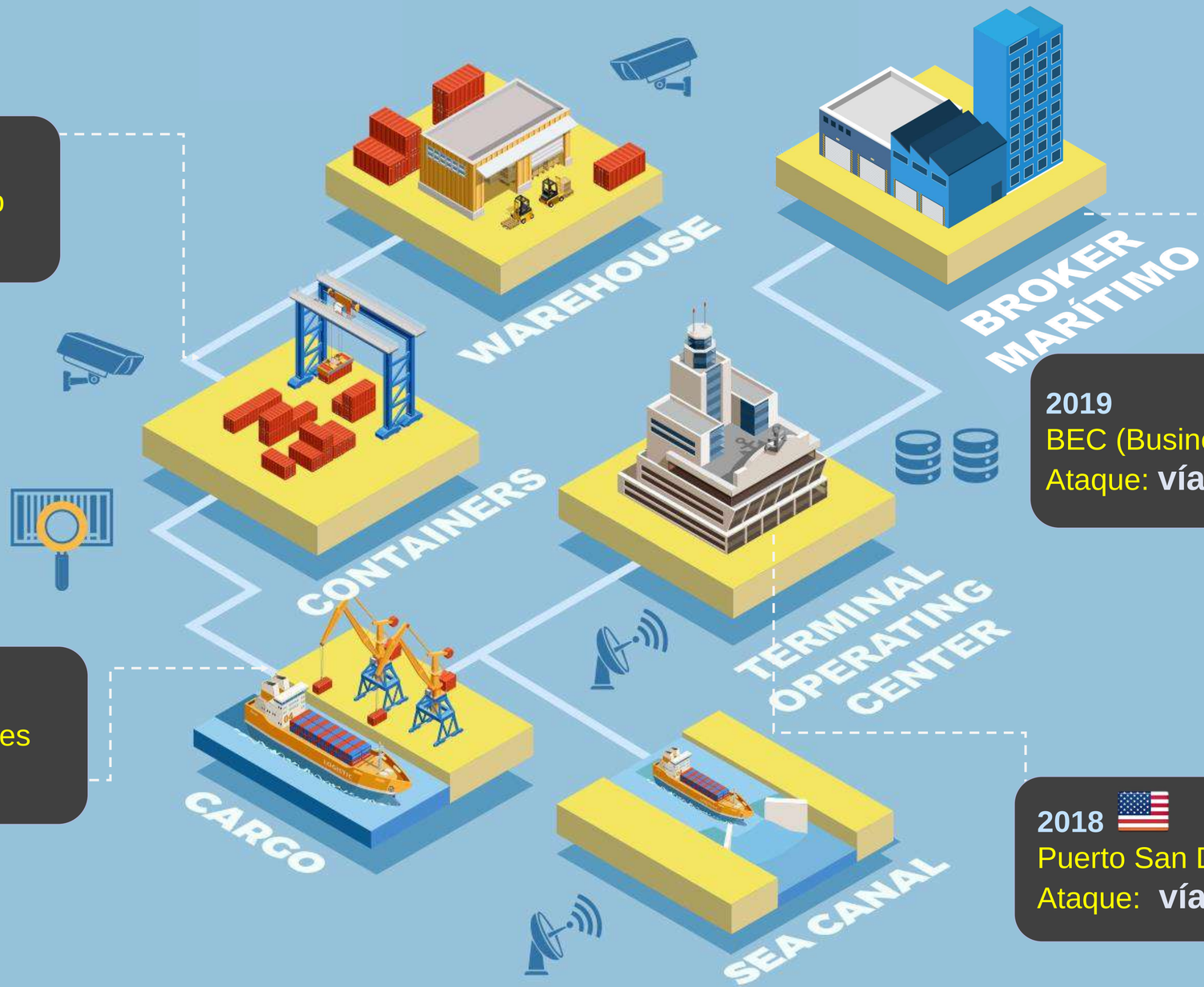


¿Qué pasa en el sector Marítimo?

Casos de ataques cibernéticos en Sector Marítimo

2013
Tráfico de drogas Puerto Antwerp
Ataque: **vía spear phishing**

2017 more
Maersk interrupción de operaciones
Ataque**: vía vulnerabilidad**



2019
BEC (Business email compromise)
Ataque: **vía ingeniería social**

2018
Puerto San Diego – secuestro de info
Ataque: **vía vulnerabilidad**

¿Qué tienen en común en estos ataques?

Información

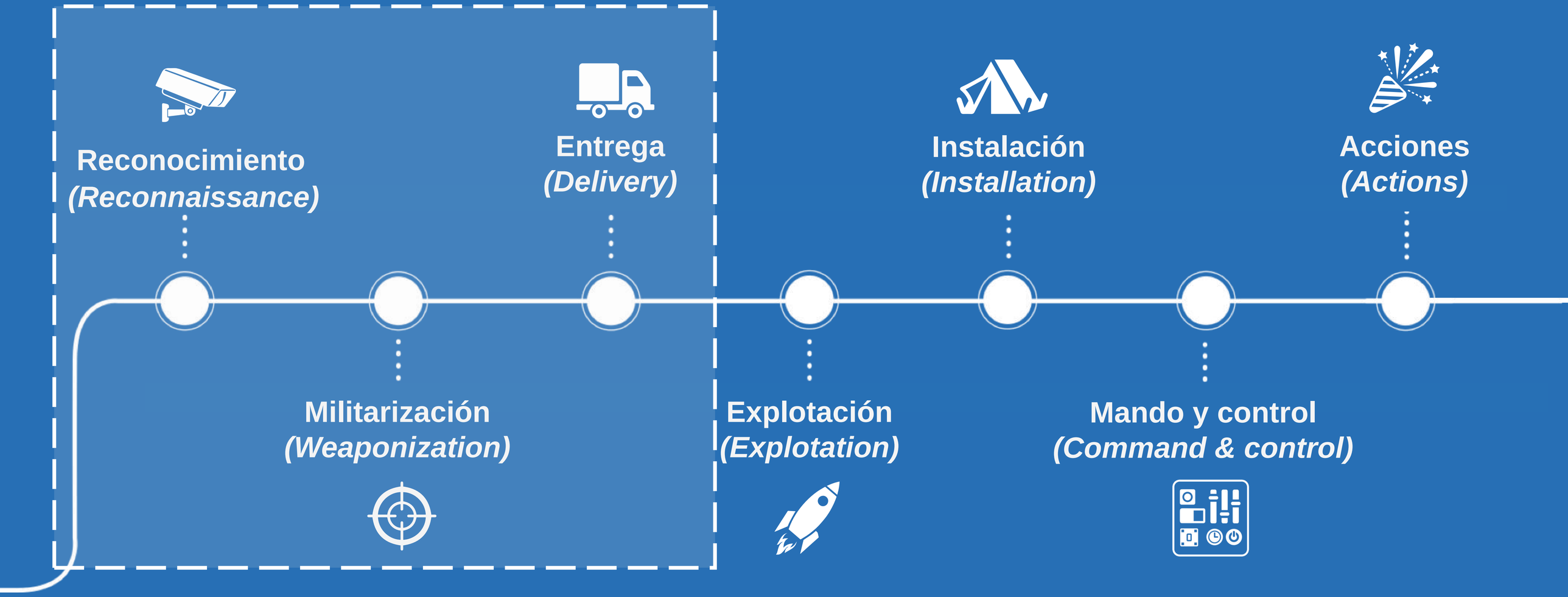
Información como insumo para un ataque

Información como premio final

Hoy en día, ¿cómo atacan a las personas y empresas?

Cyber Kill Chain

Una serie de pasos que describen cómo se lleva a cabo un ataque



Cyber Kill Chain

Una serie de pasos que describen cómo se lleva a cabo un ataque

Reconocimiento
(Reconnaissance)

Militarización
(Weaponization)

Entrega
(Delivery)

Explotación
(Explotation)

Instalación
(Installation)

Mando y control
(Command & control)

Acciones
(Actions)

Reconocimiento

¿Qué buscan?

Sitios web

Direcciones IP

Tipo de negocios

Tecnologías usadas

Correos electrónicos

Personal

Perfiles de personas

Directorios telefónicos

Dominios y subdominios

¿Dónde buscan?

Imágenes

Redes sociales

Buscadores

Servidores

Dominios y direcciones IP

Paginas web

Mapas

Foros

Comentarios

Ingeniería social

Gran aliado para la fase de reconocimiento

Reconocimiento

Ingeniería Social

Obtener información confidencial que tu **necesitas** a través de la **manipulación** de una persona

factor de éxito del ataque

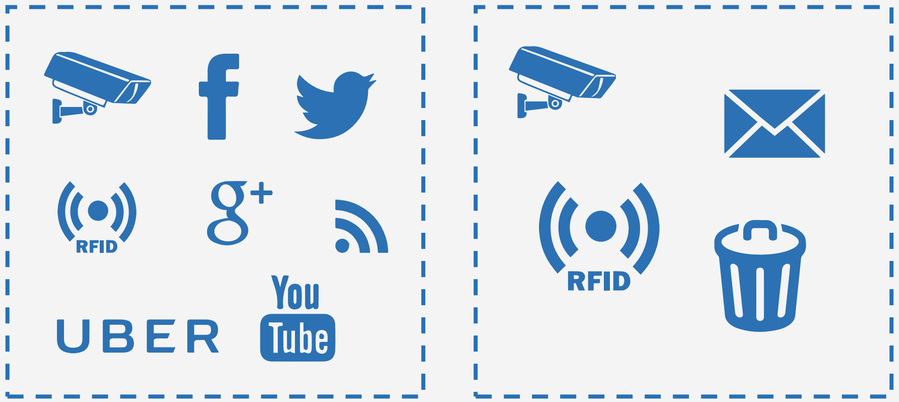
hacer que una persona confíe en ti

Como logro que confíe?

Conociendo su información

Reconocimiento

¿Qué tanta información puedo obtener de una persona?



CON INTERNET

SIN INTERNET

Conocer y manipular

Perfil
- Name/nicknames
- Current Address
- Satellite view of current address
- Citizenship
- Partido político
- Y más..

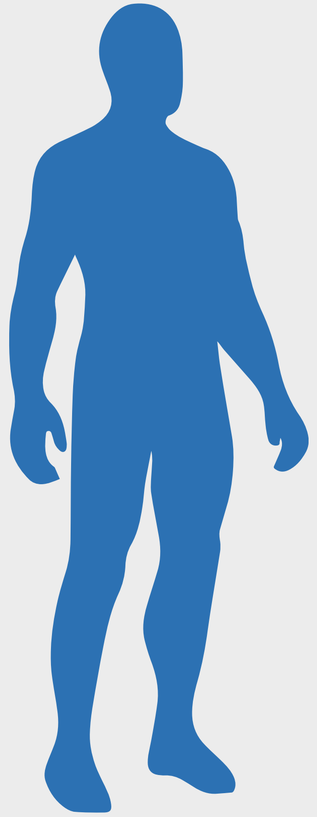
Entorno
- Pareja/hijos/abuelos
- vecinos
- Compañeros de trabajo
- Amigos redes sociales
- Personas de interés
- Y más..

Comunicaciones
- Numero teléfono
- Correos electrónicos
- Facebook/Instagram/telegram
- Buscadores
- Amigos en chat
- Websites visitados
- Y más

Estilo de vida
- Compras
- Cines/películas
- Libros
- Y más..

Finanzas
- Propiedades
- Salario actual
- Cuentas bancarias
- Credit score
- Vacaciones
- Deudas

Posición geográfica
- RFID – peajes
- GPS
- GPS del teléfono
- Fotos en redes sociales



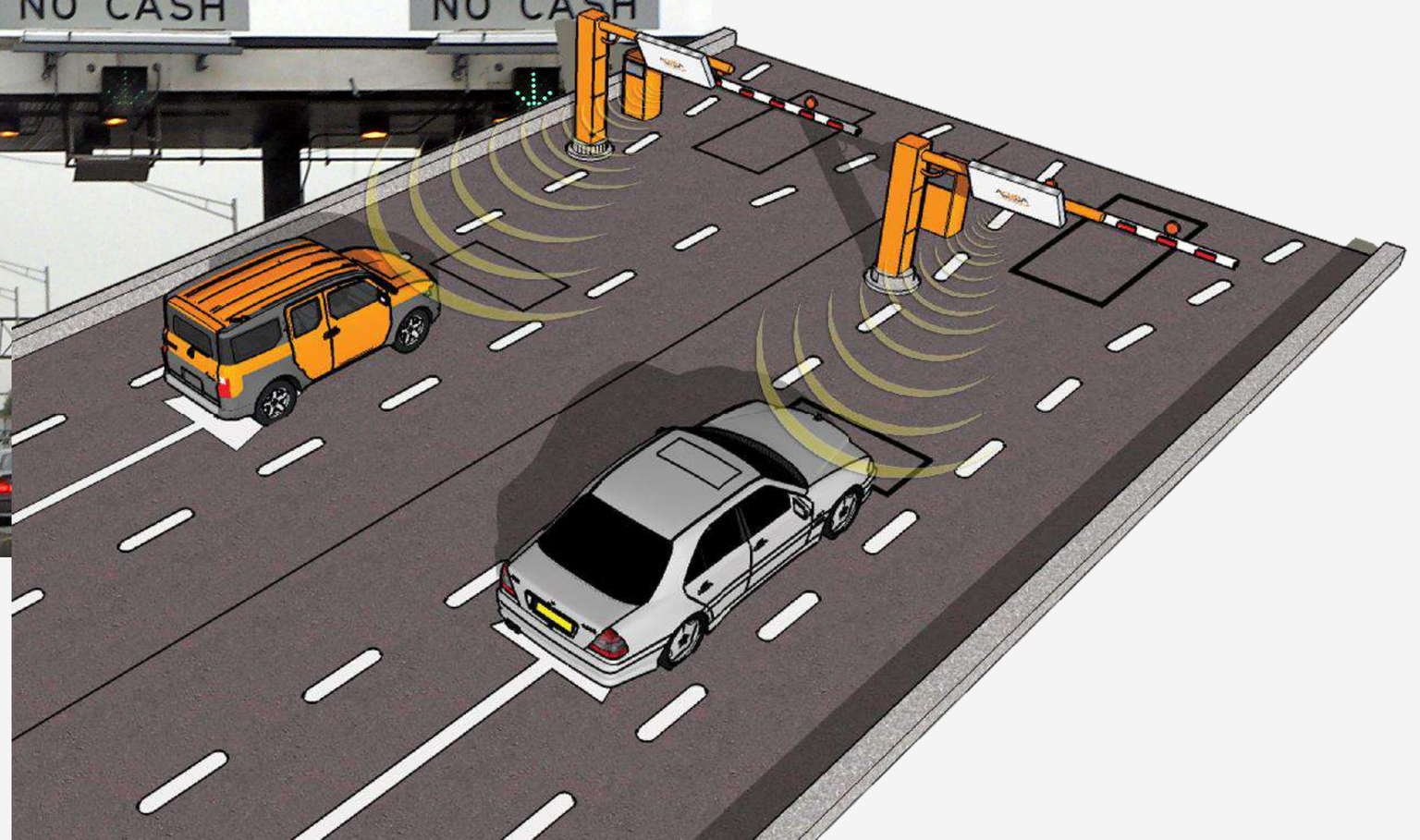
100%

0%


Sin internet

En un peaje:

Pudiera saber si fuiste al aeropuerto

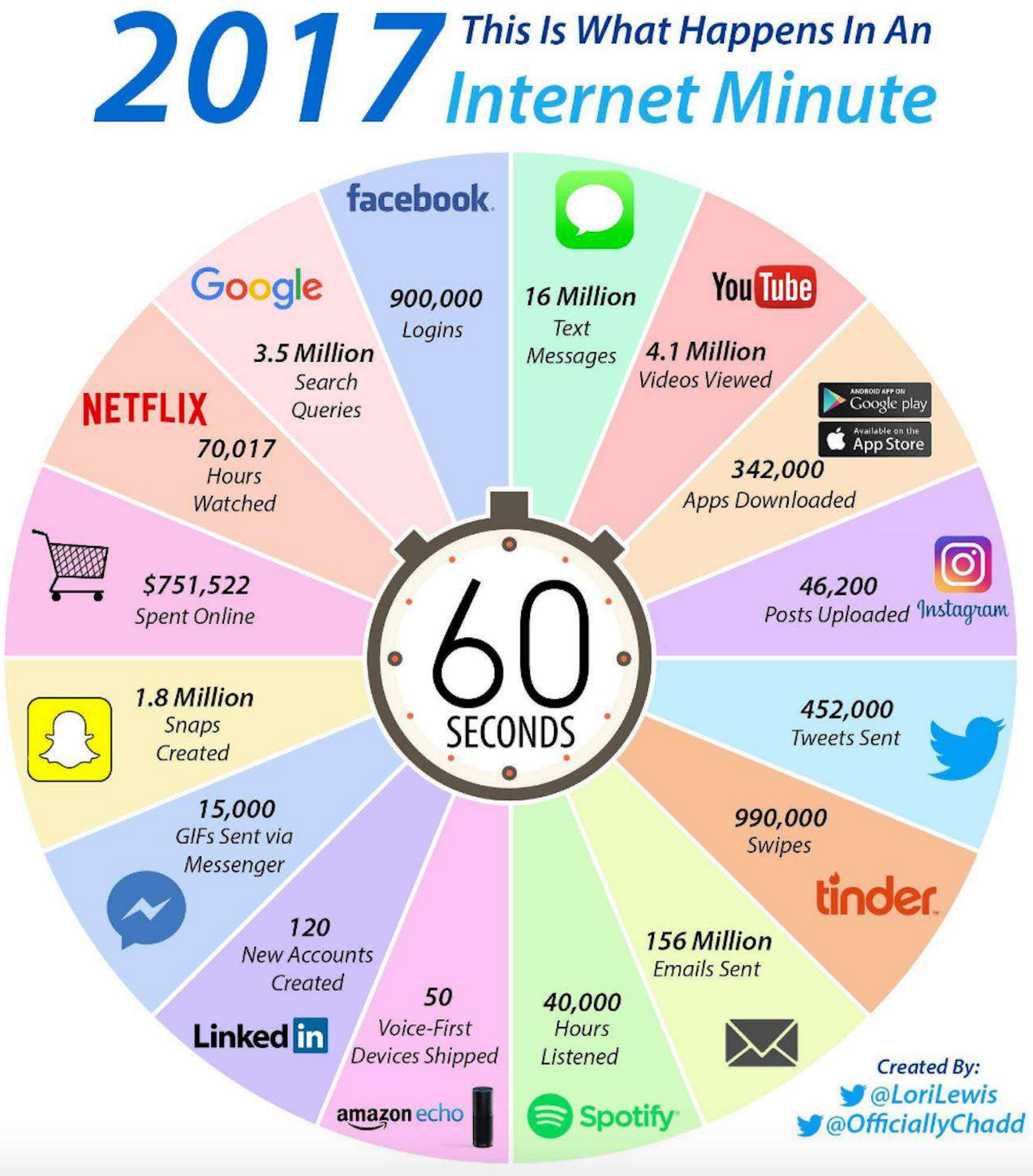


Identificación automatica de un vehiculo

RFID Identificación por radiofrecuencia


Con Internet

En 1 minuto…


2017 This Is What Happens In An Internet Minute
facebook
900,000 Logins
16 Million Text Messages
YouTube
4.1 Million Videos Viewed
342,000 Apps Downloaded
46,200 Posts Uploaded
Instagram
452,000 Tweets Sent
990,000 Swipes
tinder
156 Million Emails Sent
40,000 Hours Listened
Spotify
50 Voice-First Devices Shipped
amazon echo
120 New Accounts Created
LinkedIn
15,000 GIFs Sent via Messenger
1.8 Million Snaps Created
$751,522 Spent Online
NETFLIX
70,017 Hours Watched
Google
3.5 Million Search Queries
60 SECONDS
Created By:
@LoriLewis
@OfficiallyChadd

Por ejemplo

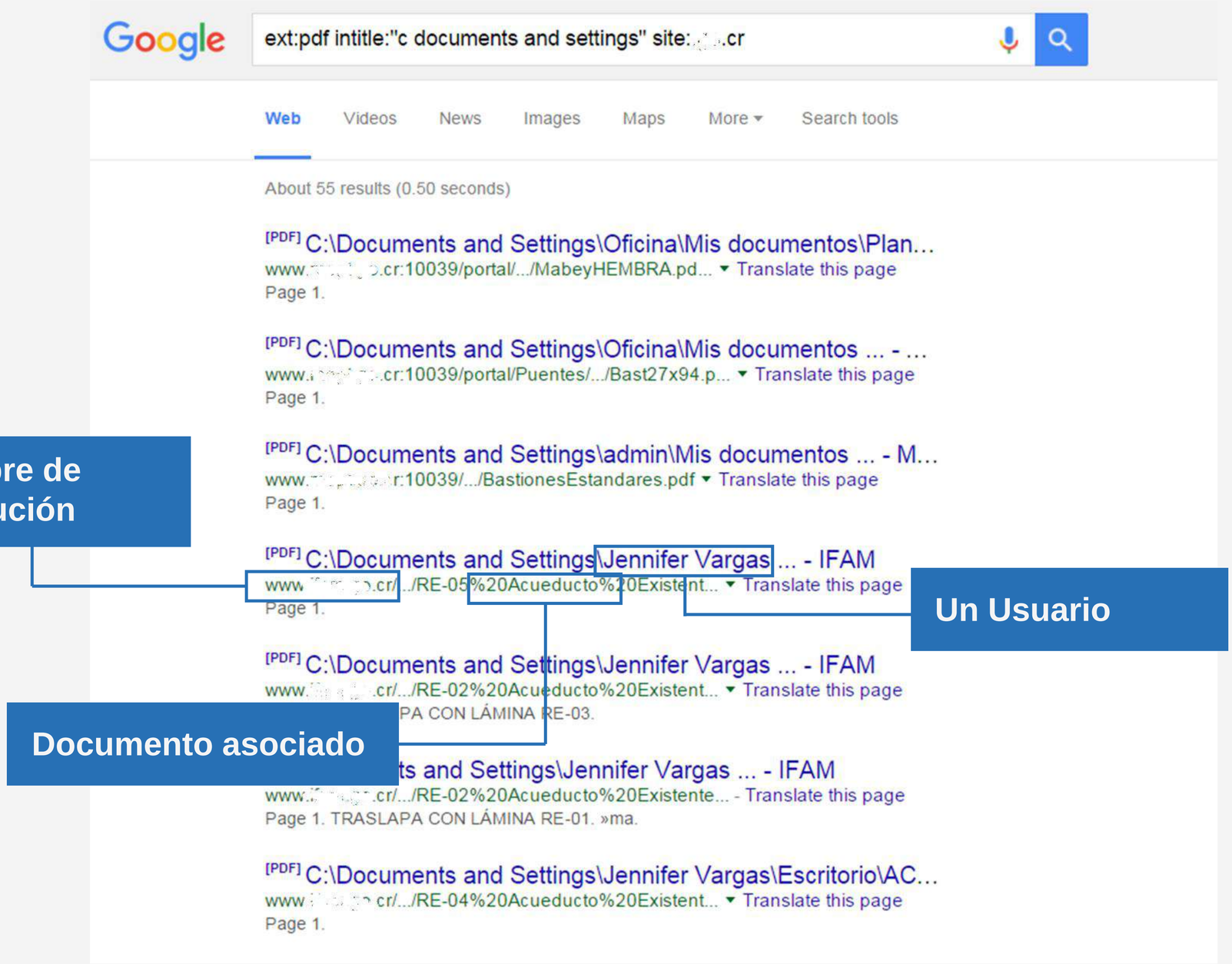
Información pública que puedo obtener con:

CON INTERNET

Reconocimiento

Búsqueda en google

Simple ejemplo para empezar a perfilar



Nombre de Institución

Documento asociado

Un Usuario

Por ejemplo

Información pública que puedo obtener con:

Por ejemplo

CON INTERNET

Reconocimiento

twitter

Aplicaciones donde revisa su cuenta twitter

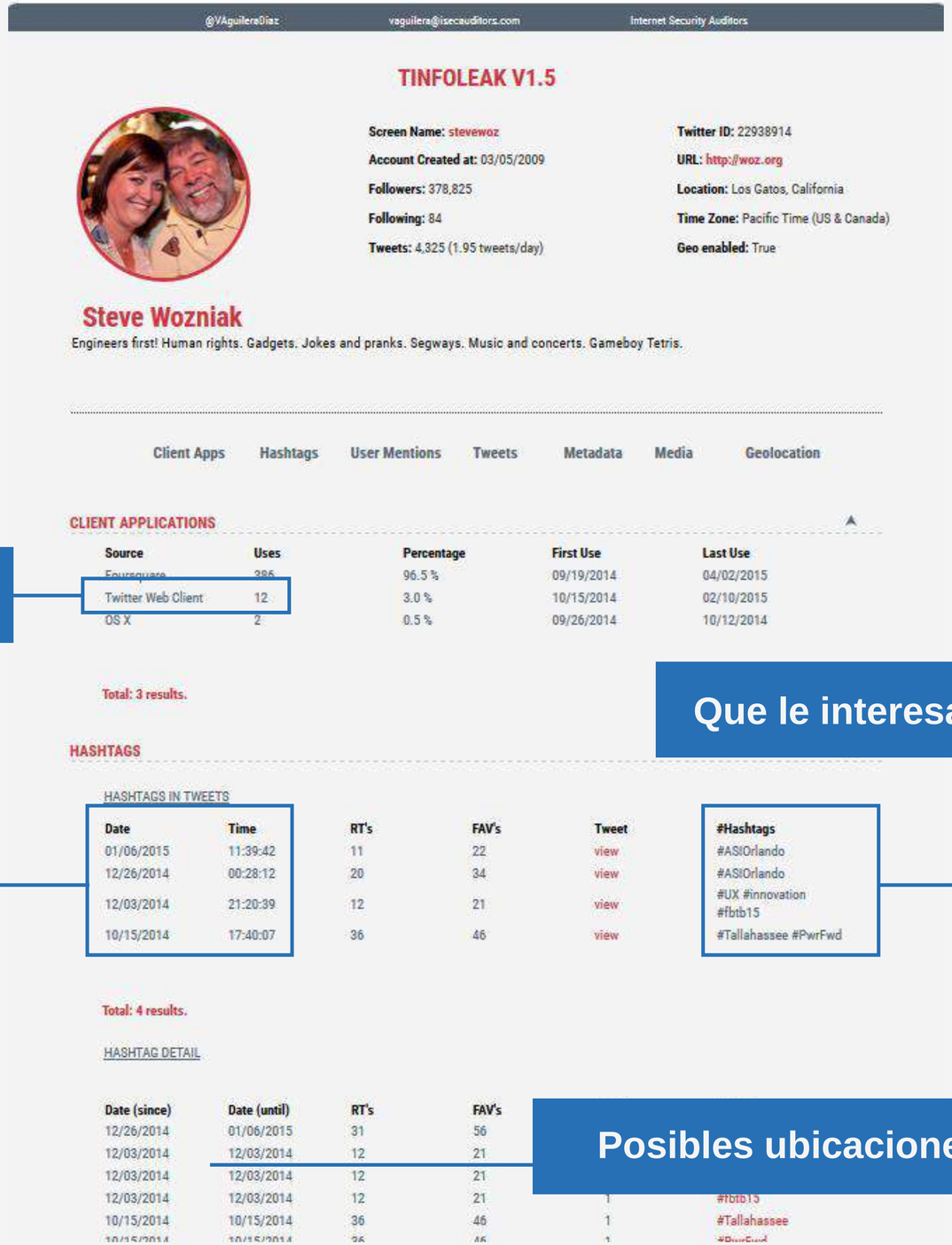
Horarios

Que le interesa en twitter

Posibles ubicaciones geográficas

Búsqueda en twitter con tinfoleak

(Herramientas libres)



@VAguileraDiaz vaguilera@isecauditors.com Internet Security Auditors

TINFOLEAK V1.5

Screen Name: stevewoz
Account Created at: 03/05/2009
Followers: 378,825
Following: 84
Tweets: 4,325 (1.95 tweets/day)
Twitter ID: 22938914
URL: http://woz.org
Location: Los Gatos, California
Time Zone: Pacific Time (US & Canada)
Geo enabled: True

Steve Wozniak

Engineers first! Human rights. Gadgets. Jokes and pranks. Segways. Music and concerts. Gameboy Tetris.

Client Apps | Hashtags | User Mentions | Tweets | Metadata | Media | Geolocation

CLIENT APPLICATIONS

Source	Uses	Percentage	First Use	Last Use
Foursquare	386	96.5 %	09/19/2014	04/02/2015
Twitter Web Client	12	3.0 %	10/15/2014	02/10/2015
OS X	2	0.5 %	09/26/2014	10/12/2014

Total: 3 results.

HASHTAGS

HASHTAGS IN TWEETS

Date	Time	RT's	FAV's	Tweet	#Hashtags
01/06/2015	11:39:42	11	22	view	#ASIOrlando
12/26/2014	00:28:12	20	34	view	#ASIOrlando
12/03/2014	21:20:39	12	21	view	#UX #innovation #fbtb15
10/15/2014	17:40:07	36	46	view	#Tallahassee #PwrFwd

Total: 4 results.

HASHTAG DETAIL

Date (since)	Date (until)	RT's	FAV's		
12/26/2014	01/06/2015	31	56		
12/03/2014	12/03/2014	12	21		
12/03/2014	12/03/2014	12	21		
12/03/2014	12/03/2014	12	21	1	#fbtb15
10/15/2014	10/15/2014	36	46	1	#Tallahassee

Con solo información pública colectada de:

Casos típicos pero efectivos:

El falso Soporte técnico

Cyber Kill Chain

Reconocimiento — **Militarización** — **Entrega**

01

Hola “**xxxx**”, te llama **“XXX”** del departamento de tecnología para el control de estándares y seguridad perimetral del banco **xxx**, hay un problema con un documento que editaste llamado **“xxx”** te mandare un correo con el **link** para que lo revises de inmediato…

Departamento de finanzas

02

Elabora y **envía “código malicioso”**

Departamento de finanzas

Cyber Kill Chain

Una serie de pasos que describen cómo se lleva a cabo un ataque

Reconocimiento
(Reconnaissance)

Militarización
(Weaponization)

Entrega
(Delivery)

Explotación
(Explotation)

Instalación
(Installation)

Mando y control
(Command & control)

Acciones
(Actions)

Militarización
(Weaponization)

Preparan operación y armas

Conociendo perfiles y vulnerabilidades en plataforma tecnológica de una empresa..

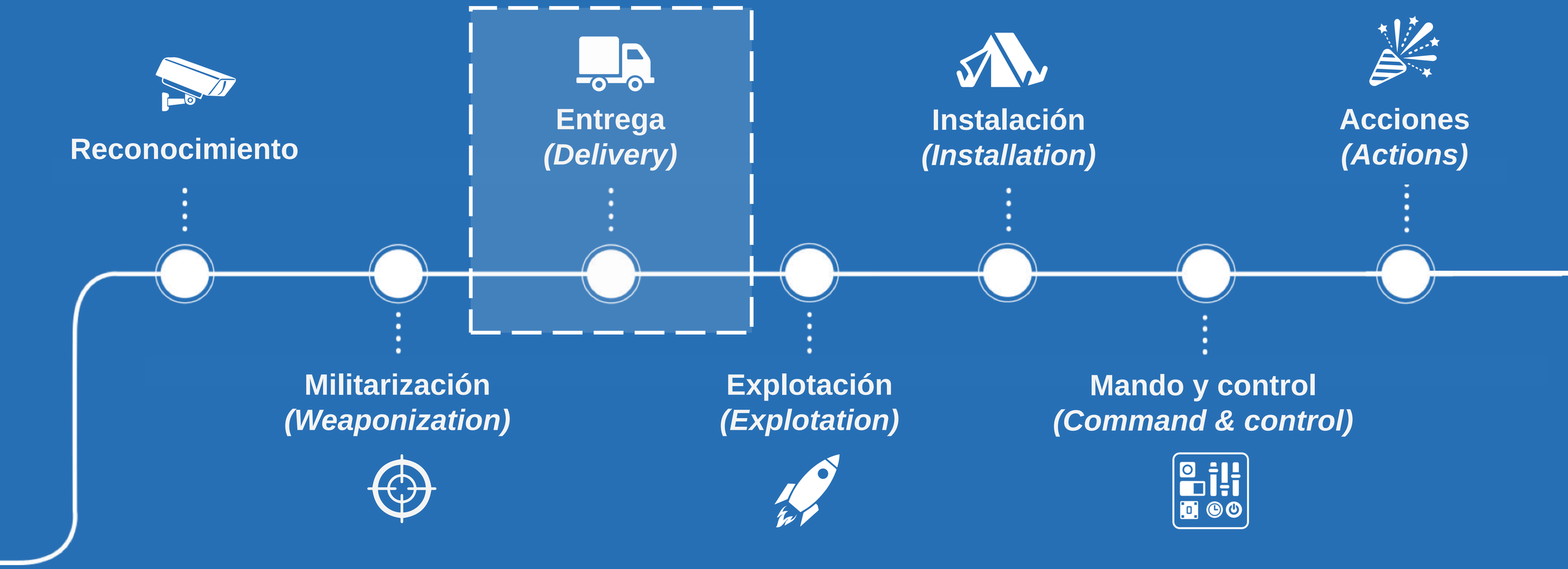
Ransomware

Troyano

Malware

Cyber Kill Chain

Una serie de pasos que describen cómo se lleva a cabo un ataque



Entrega
(Delivery)

Transporte del ataque

Email link

USB

Sitio malicioso

Cyber Kill Chain

Una serie de pasos que describen cómo se lleva a cabo un ataque

Reconocimiento
(Reconnaissance)

Militarización
(Weaponization)

Entrega
(Delivery)

Explotación
(Explotation)

Instalación
(Installation)

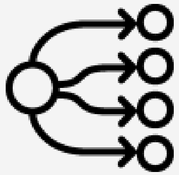
Mando y control
(Command & control)

Acciones
(Actions)

Explotación
(Explotation)

Explotación de vulnerabilidad

Bypass en controles...



Puertos

Software vulnerable

Debilidad en Password

Cyber Kill Chain

Una serie de pasos que describen cómo se lleva a cabo un ataque

Reconocimiento
(Reconnaissance)

Militarización
(Weaponization)

Entrega
(Delivery)

Explotación
(Explotation)

Instalación
(Installation)

Mando y control
(Command & control)

Acciones
(Actions)

Ataques a empresas comunes en 2019 en la región

Ransomware

Your money
or your *data*

¿Cómo opera?

Inyectar código

Secuestrar info

Esperar pago

Ataques BEC

(Business email compromise)

Ataques BEC

Principal Objetivo

Dominio Marítimo entre lo mas rentables para ataques BEC

Atractivos para ataques #BEC en el sector Marítimo

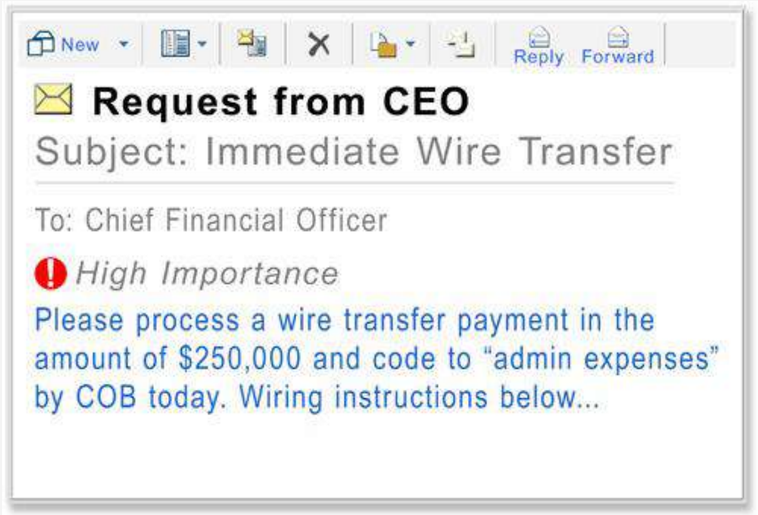
El día y la noche
Trabajan con muchas zonas horarias

Elevada cantidad de transacciones
Mucho dinero en movimiento

Interacción impersonal
Una gran mayoría se maneja por correo electrónico

Métodos comunes BEC

CEO Fraud



Se compromete la cuenta del jefe / líder / dueño

Recibe correo del “falso” del jefe. Envía el pago a la cuenta del ladrón.

Espera el dinero

- Email link
- Social network
- Email attachment

Métodos más comunes BEC

The Bogus Invoice Scheme

Se compromete la cuenta de un empleado.

Recibe correo con un cambio de cuenta. Envía el pago a la cuenta del ladrón.

Espera el dinero

- Email link
- Social network
- Email attachment

Ataque Formjacking

Robo de información de tarjetas de crédito vía pasarelas de pago


CASH

Formjacking

Principales blancos de ataque:

Cualquier sitio que acepte pagos en línea

- Brokers marítimos
- Alquiler de autos
- Hoteles
- Tiendas departamentales
- Etc.

Objetivo:

Robar Información de tu tarjeta de crédito

Formjacking

Que inyecta?

Código malicioso JavaScript para robar data de tarjetas de créditos

Patrones comunes?

En pasarelas de pago

```
<li><a href="/prop65">Prop. 65</a></li>
</ul>
<script src="https://www.zoobashop.com/media/js/js.js"></script>

                    <div class="social">
                     <div class="social">
        <ul>
```

Casos recientes

- Ticket Master
- British Airways
- Feedify
- Newegg

Source: Symantec

¿Por qué son tan exitosos los ataques a las empresas?

Aumento en conectividad

10 años antes

10 años después

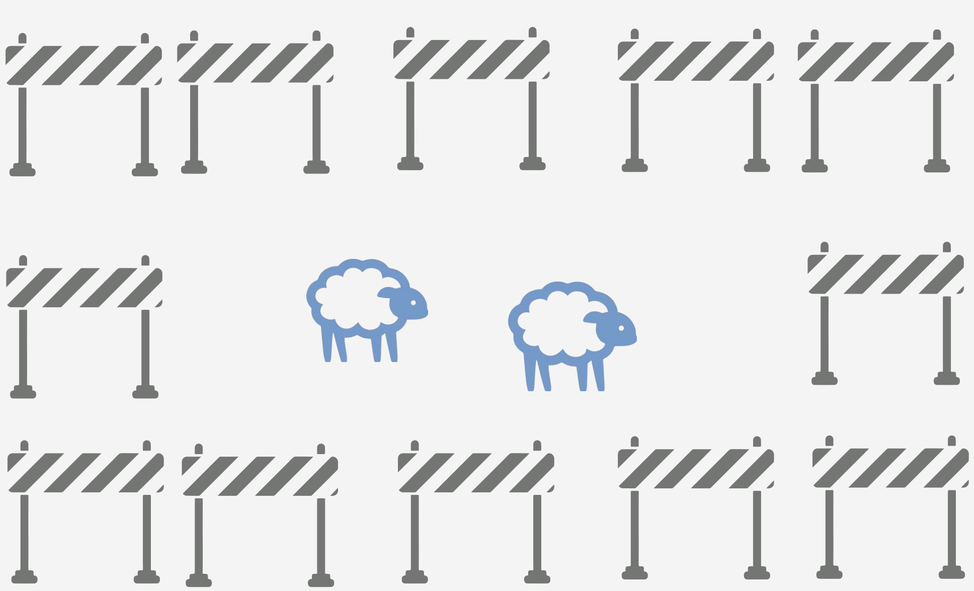
Consolidación IT

10 años antes

10 años después

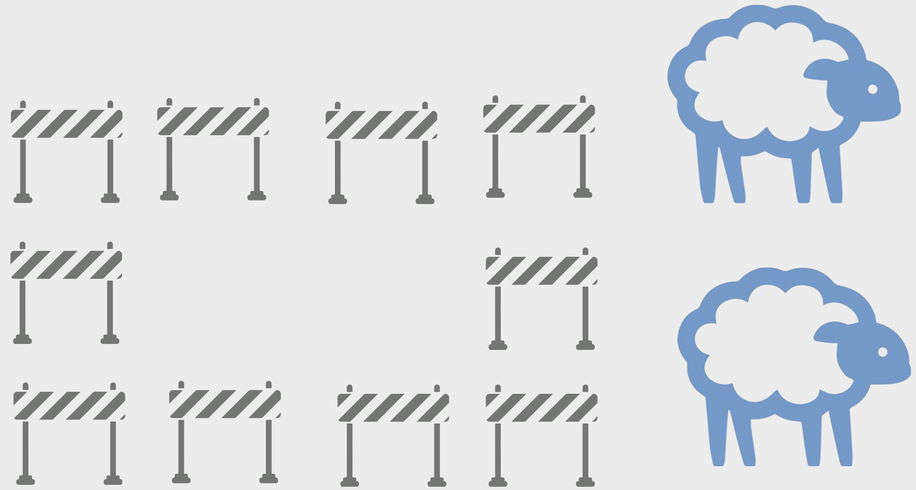
Fracasos en controles preventivos

10 años antes



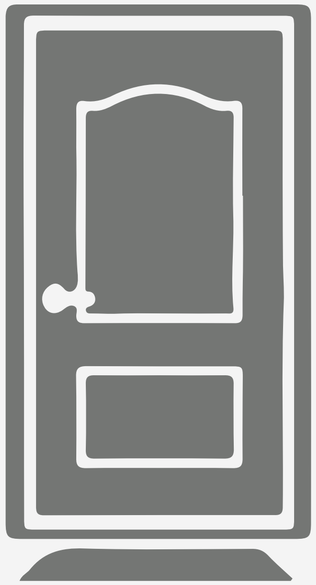
Password de 6 carácteres

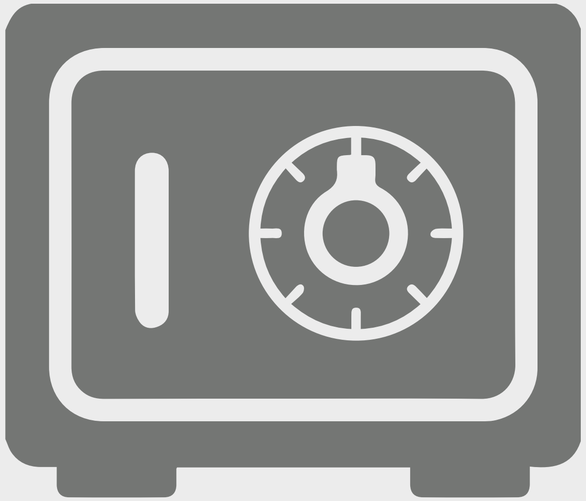
10 años después



Password de 6 carácteres

Cumplimiento / Capacidad





Cumplimiento: presencia o ausencia

Nuevos métodos para la ciberdefensa de las empresas

Nuevas formas de ciberdefensa

Asumir que el atacante es **inteligente** y **saltará** todas tus barreras preventivas

Diseñar defensas para detectar y retrasar el ataque y dar tiempo a los defensores

Defensas que mitiguen y suministren redundancia en la protección

Mecanismos de defensa para capturar y rechazar el ataque

Después que comience pero **antes que de sea exitoso**

Thank you!
Merci
Gracias
Obrigado

Diego Subero

OAS Cybersecurity Program
Organization of American States

cybersecurity@oas.org

@OEA_Cyber