Tilsor

Ciber Inteligencia para Aplicaciones Web

Ing. Gustavo Betarte, PhD
Ing. Rodrigo Martínez

JIAP - Octubre 2016

Tilsor

Agenda

- Contexto
- Tipos de ataques y cifras
- Ciber inteligencia
- WAFINTL

Tilsor

Contexto

JIAP - Octubre 2016

Tilsor

CSIRT Tilsor

Comunidad Objetivo

- Socios tecnológicos y clientes de Tilsor S.A.
- SGSI de Tilsor S.A.

CSIRT Tilsor
Equipo de Respuesta a Incidentes de Seguridad Informática

Visión/Misión

- Ser un equipo de referencia en la gestión de incidentes y el asesoramiento de mejores prácticas en seguridad informática
- Coordinar en forma eficaz la gestión y respuesta de incidentes de seguridad
- Brindar asistencia en forma proactiva
- Capacitar y promover acciones de sensibilización
- Relacionarse con equipos pares y con la comunidad, difundiendo alertas de seguridad y vulnerabilidades detectadas

ISO 27001:2005
REG: SGSI 8/01
LSQA
LATU+QUALITYAUSTRIA

Tilsor

Preámbulo

JIAP - Octubre 2016

Tilsor

Activos, riesgos y escenarios tecnológicos

- La digitalización de los activos corporativos ha sido acompañada por una digitalización de los riesgos corporativos
  - Pérdida de Propiedad Intelectual, Destrucción o alteración de los datos, Daño a la reputación, Fallo de infraestructura crítica, Sanciones legales y/o regulatorias, etc.

- Convergencia
  - Interconexión de sistemas internos
  - Interdependencia con sistemas externos

- Consecuencias
  - Exposición de los sistemas (de infraestructuras críticas) a potenciales ataques de Internet
  - Nuevos riesgos: conexiones *wireless*, mantenimiento remoto por terceros, nubes

Tilsor

Criticidad de ciber-ataques

- Ciber-ataques y fallos en sistemas de las infraestructuras críticas se encuentran en el Top 5 de riesgos globales según el WEF (World Economic Forum)

- En últimos 5 años el número de amenazas cibernéticas se ha multiplicado de manera exponencial

- Algunas estimaciones predicen que entre 9 y 21 billones de USD de valor económico global podrían estar en riesgo si los gobiernos y las empresas no son capaces de combatir las ciber-amenazas

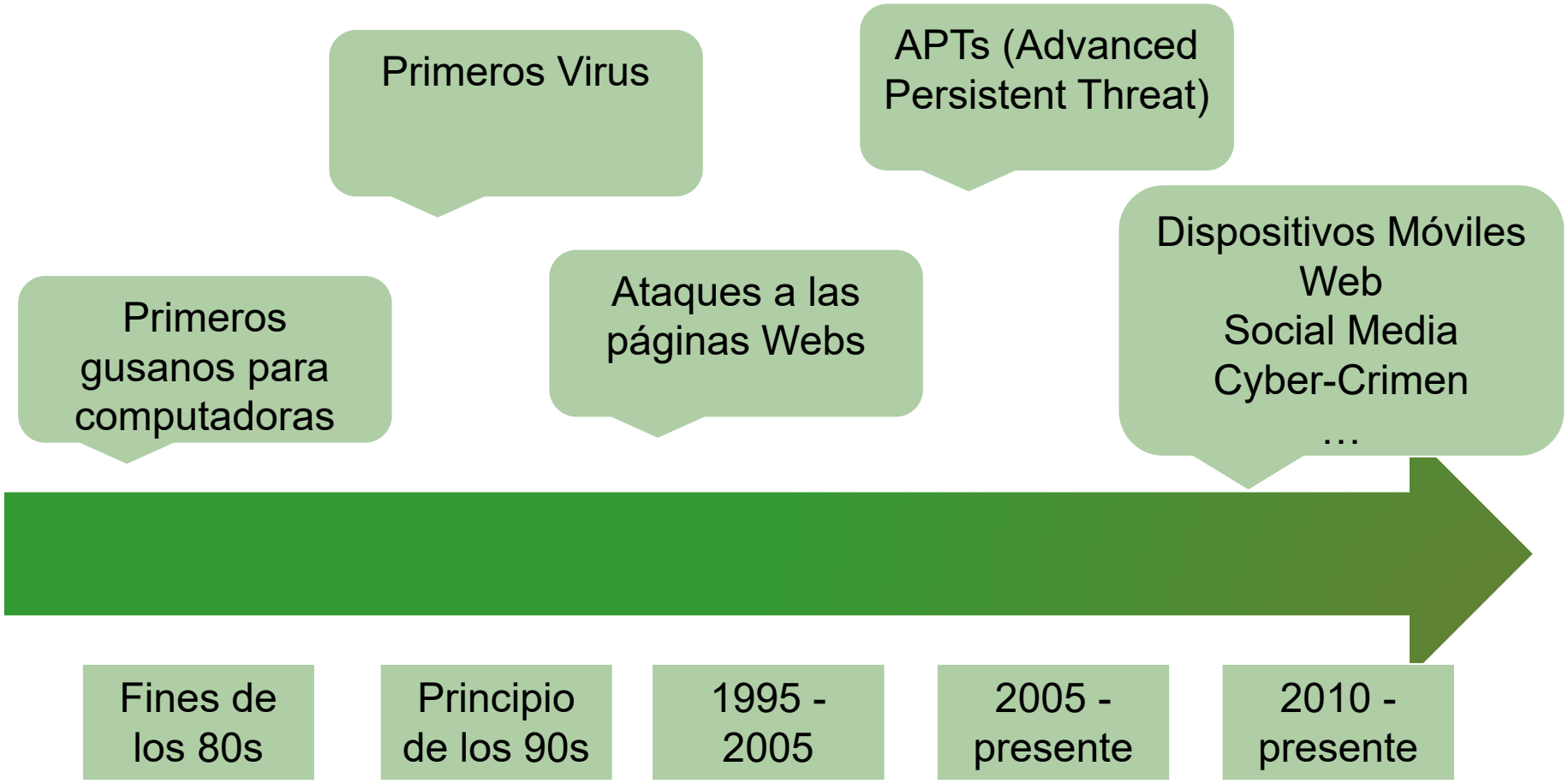
Tilsor

Tipos de ataques y algunas cifras

JIAP - Octubre 2016

Tilsor

Un poco de historia - Evolución



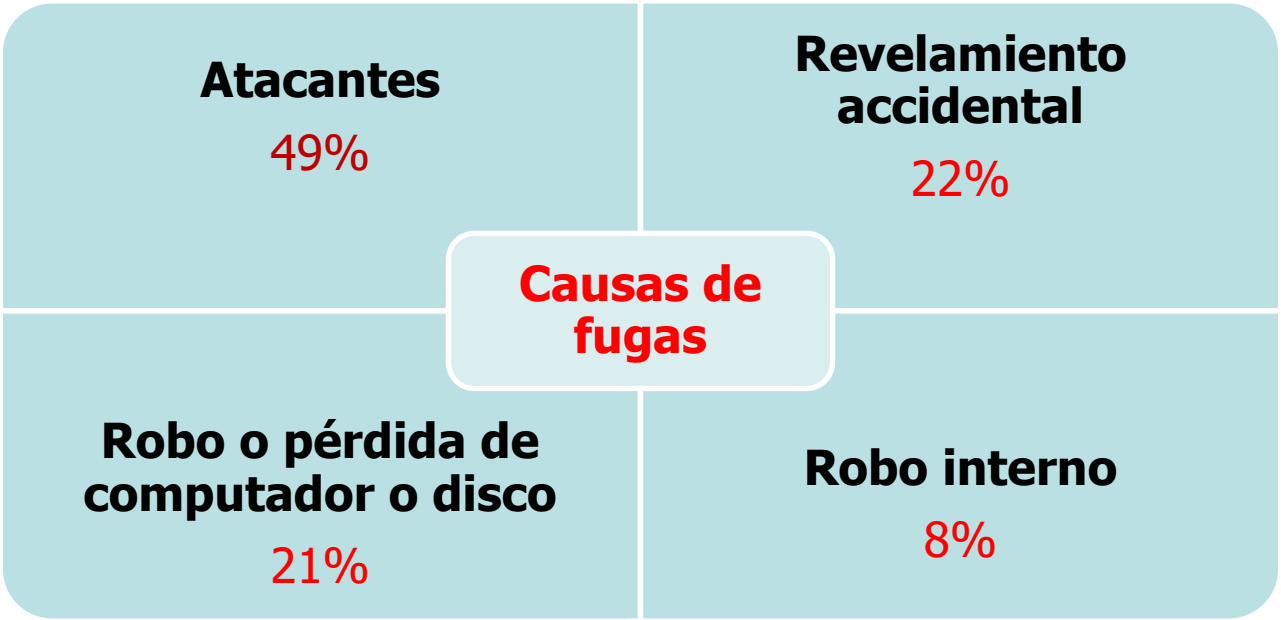
Tilsor

Web

- Vulnerabilidades
  - (2014) Heartbleed, Shellshock, Poodle
  - … en total se detectaron 6.549
- 75% de websites escaneados por Symantec en 2014 tenían vulnerabilidades, 20% de ellas críticas
- Nuevas tendencias:
  - Malvertising
  - Ransomware
- Según informe de Neustar, en 2013 60% de las compañías sufrieron un ataque de DDoS
  - Symantec constató 183% de incremento en ataques de amplificación de DNS

Tilsor

Fuga de datos y privacidad



Tilsor

Ciber-crimen & Malware
Ransomware

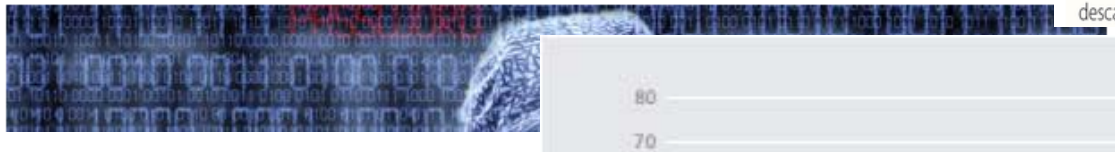
www.elpais.com.uy/vida-actual/secuestro-rescate-archivos.html

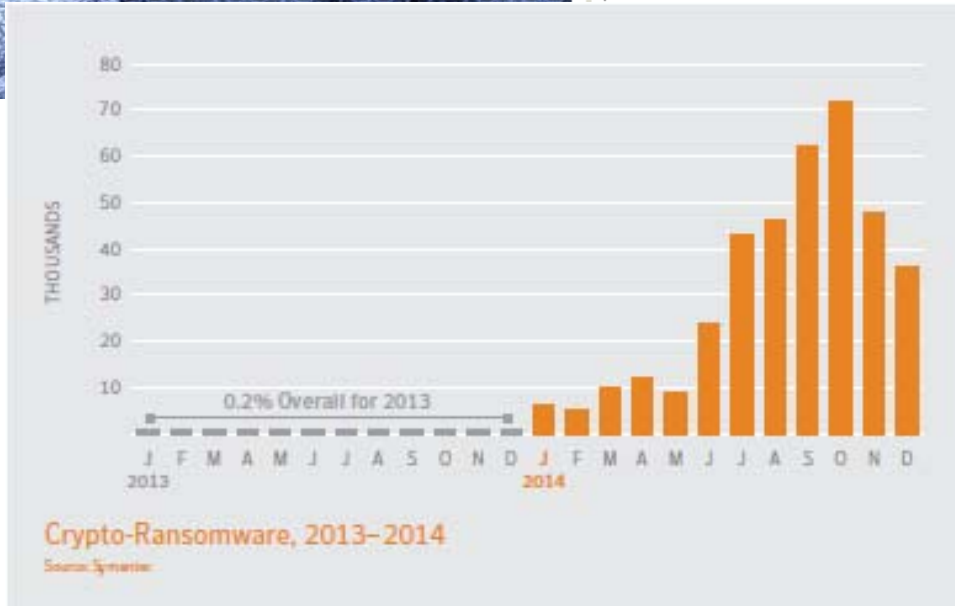
UNA EMPRESA URUGUAYA PAGÓ 2.000 DÓLARES POR RECUPERAR SUS DATOS

Secuestro y rescate de archivos

Una empresa privada uruguaya pagó 2.000 dólares para lograr un rescate de sus archivos digitales, luego de que su computadora fue secuestrada, informó a El País Santiago Paz, dir del Centro de Respuesta a Incidentes de Seguridad Informática de Uruguay (CERTuy).

FOTO





Tilsor

Ciber inteligencia

JIAP - Octubre 2016

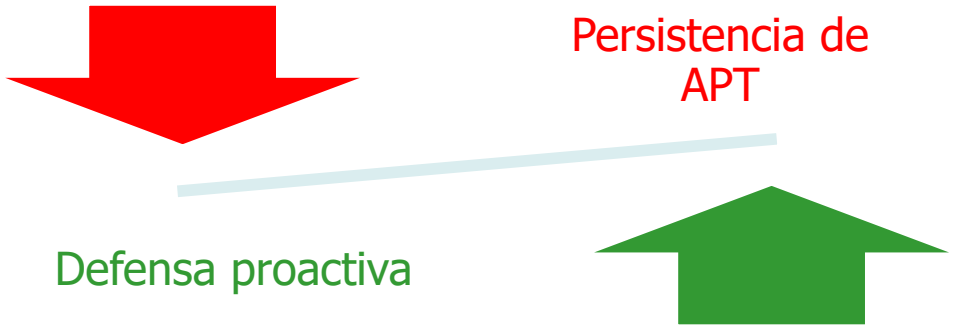
Tilsor

APT: un modelo emergente de ataques

- Antes
  - Amenaza de redes de computadoras era código auto-propagante
- Ahora
  - Secuencia de intrusiones guiadas por fallas y éxitos
  - Explotación de diferentes vulnerabilidades y combinación de ataques
  - Tienden a persistir dentro de la infraestructura de la organización
  - Los afectados raramente saben que son objetivo de ataque y desconocen origen del mismo
  - Defensa no puede ser (sólo) reactiva

Tilsor

Kill chain



Tilsor

Ciber inteligencia

- Busca entender
  - Qué tipo de ataques han ocurrido y pueden ocurrir
  - Cómo estos ataques pueden ser detectados y reconocidos
  - Cómo pueden ser mitigados?
- y caracterizar
  - Cuáles son los actores maliciosos relevantes
  - Cuáles son sus objetivos y sus capacidades (TTP)
  - Qué vulnerabilidades, configuraciones incorrectas o debilidades son sus más probables objetivos
  - Qué acciones han tomado en el pasado

Tilsor

WAFINTL

Técnicas y Herramientas para el desarrollo de Ciber inteligencia en Aplicaciones Web

JIAP - Octubre 2016

Tilsor

ICT4V (http://www.ict4v.org)

- Centro de investigación e innovación multidisciplinario en el campo de las TIC y sus aplicaciones a los sectores verticales, como ser energía, agro, bancario y salud, entre otros
- Combina capacidades de investigación e innovación de América Latina, Europa y Norteamérica
- Asociación abierta entre empresas, universidades, centros de investigación y agencias públicas
- Desarrolla proyectos y brinda servicios a sus socios y a empresas y organismos externos
- Incorpora en un mismo espacio personal altamente calificado de diversos perfiles y disciplinas, investigadores, expertos y emprendedores del más alto nivel, del centro e invitados de distintos continentes

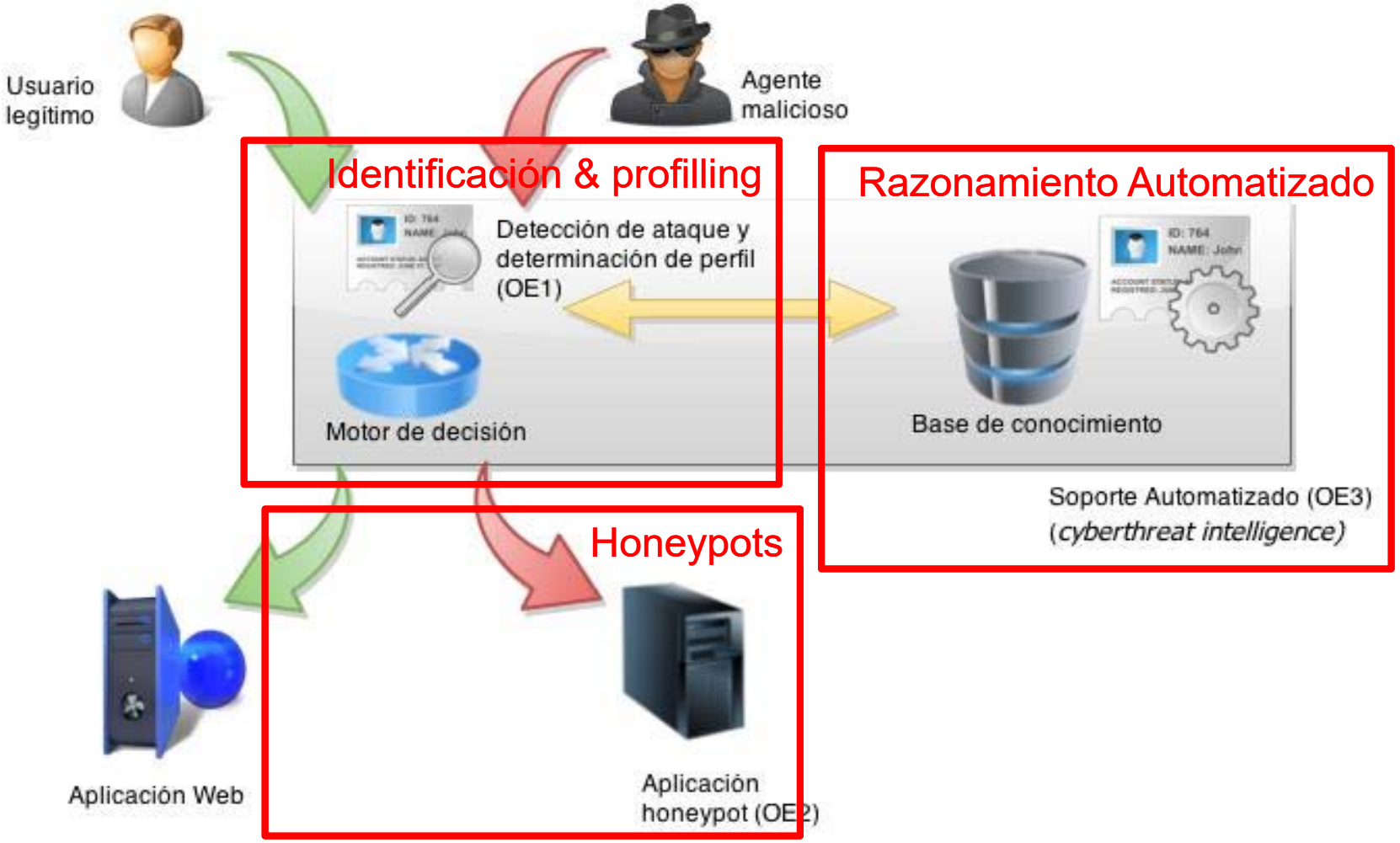
Tilsor

El Problema

- Vulnerabilidad de aplicaciones web
- Drástico incremento de ataques informáticos
- Impacto en las organizaciones
- Ciber seguridad clásica (reactiva) ya no es suficiente: APTs
- Ciber inteligencia

Tilsor

El Proyecto



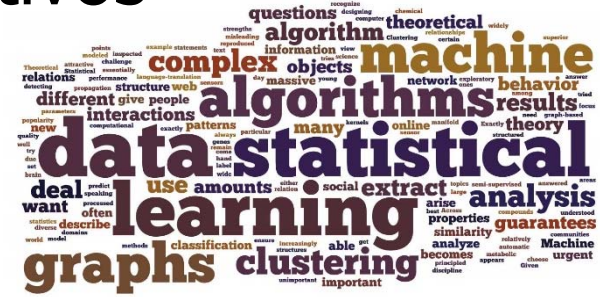
Tilsor

Los avances – OE1

- Tecnologías
  - ModSecurity
  - OWASP CRS

modsecurity
Open Source Web Application Firewall

- Uso de Inteligencia Artificial
  - Identificación de ataques
  - Disminución de Falsos Positivos



Tilsor

Resultados

- ModSecurity + OWASP CRS
  - Precisión: 0,93
  - Sensibilidad: 0,74
  - Exactitud: 0,78

Matriz de Confusión	
25797	8841
1938	12431

- MAA + Information Retrieval
  - Precisión: **0,99**
  - Sensibilidad: **0,98**
  - Exactitud: **0,99**

Matriz de Confusión	
34868	138
307	14803

Tilsor

Preguntas?

Tilsor

Muchas gracias

JIAP - Octubre 2016