



wpnicaragua.org



WordPress Meetup Managua

The background image shows a panoramic view of the city of Managua, Nicaragua. In the foreground, there's a dense area of green trees. Beyond them, the city's skyline is visible, featuring several buildings of varying heights, including a prominent tall skyscraper with a grid-like facade. A flag is flying from a pole on top of one of the buildings. The sky above the city is a clear, pale blue.

BIENVENIDOS!

Una charla de
Salvador Aguilar
@riper81

sal.aguilar81@gmail.com
salrocks.wordpress.com

Organización de esta charla

1. ¿Quién es Salvador Aguilar?
2. ¿Para quien es esta charla?
3. Estadísticas generales
4. Tipos de infección & los impactos
5. Un ambiente complejo
6. Tipos de ataques
7. Flujo de los ataques
8. Vectores de ataque
9. ¿Pensando sobre seguridad?
10. Preguntas y respuestas

Quién es Salvador Aguilar?



- Papá de un niño de 8 y una niña de 1.5 años.
- Entusiasta de Wordpress.
- Con experiencia trabajando para empresas como SEARS Mexico, Site5.com & Sucuri.net
- Analista de seguridad en Sucuri.net
- **Implementador** de Wordpress
- CoFundador & SysAdmin de SenorCoders.com

Para quien es esta charla?

- Para cualquier persona que tiene un sitio web
- Para profesionales que diseñan sitios web
- Para personas que han sido infectadas
- Para personas que tienen su sitio web en una lista negra
- Para personas que quieren saber como los hackiaron
- Para personas que quieren saber sobre los diferentes vectores de ataque



Estadísticas Generales

ABRIL 2016 = 1.02 Billones de Sitios Web

Sitios web con CMS

33%



Cobertura de CMS

73%



Estadísticas sobre Wordpress

MOTOR DE

25%

LA WEB

EL CMS + POPULAR

59%

VS LOS DEMAS

MUCHOS PLUGINS

42000+

Gratis y más de 100
Plugins PREMIUM

Estadísticas de Infecciones: Enero – Marzo 2016

11,000 Sitios Web infectados

75% → Wordpress (8250)

50% Wordpress Desactualizados



+80% Sitios web infectados → desactualizados

Estadísticas de Google

50 Millones de Warnings

20,000

Sitios web x semana en
Lista Negra x Malware

50,000

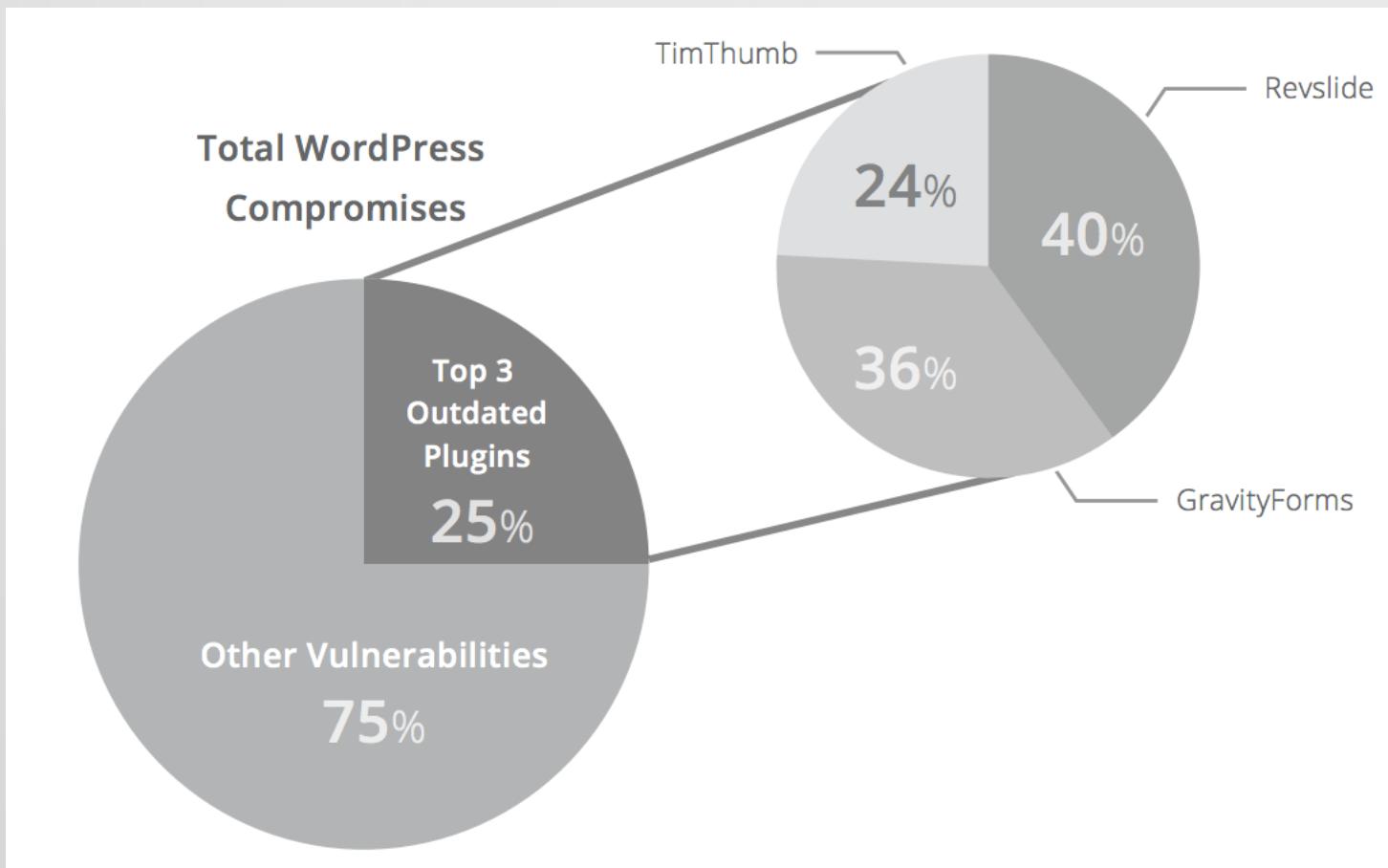
Sitios web x semana en
Lista Negra Phishing



95%

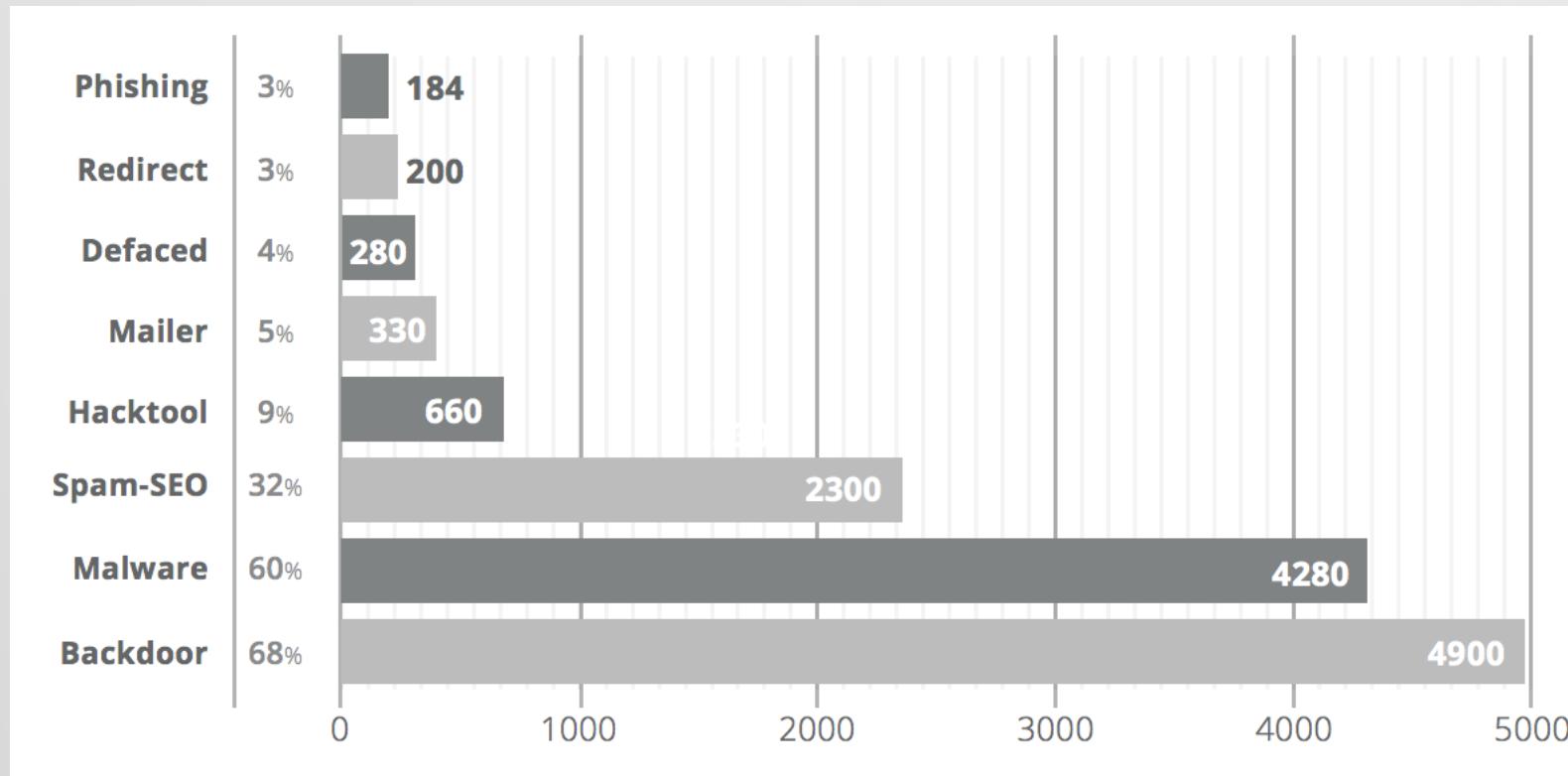
Reducción
de tráfico

Estadísticas sobre Plugins de Wordpress

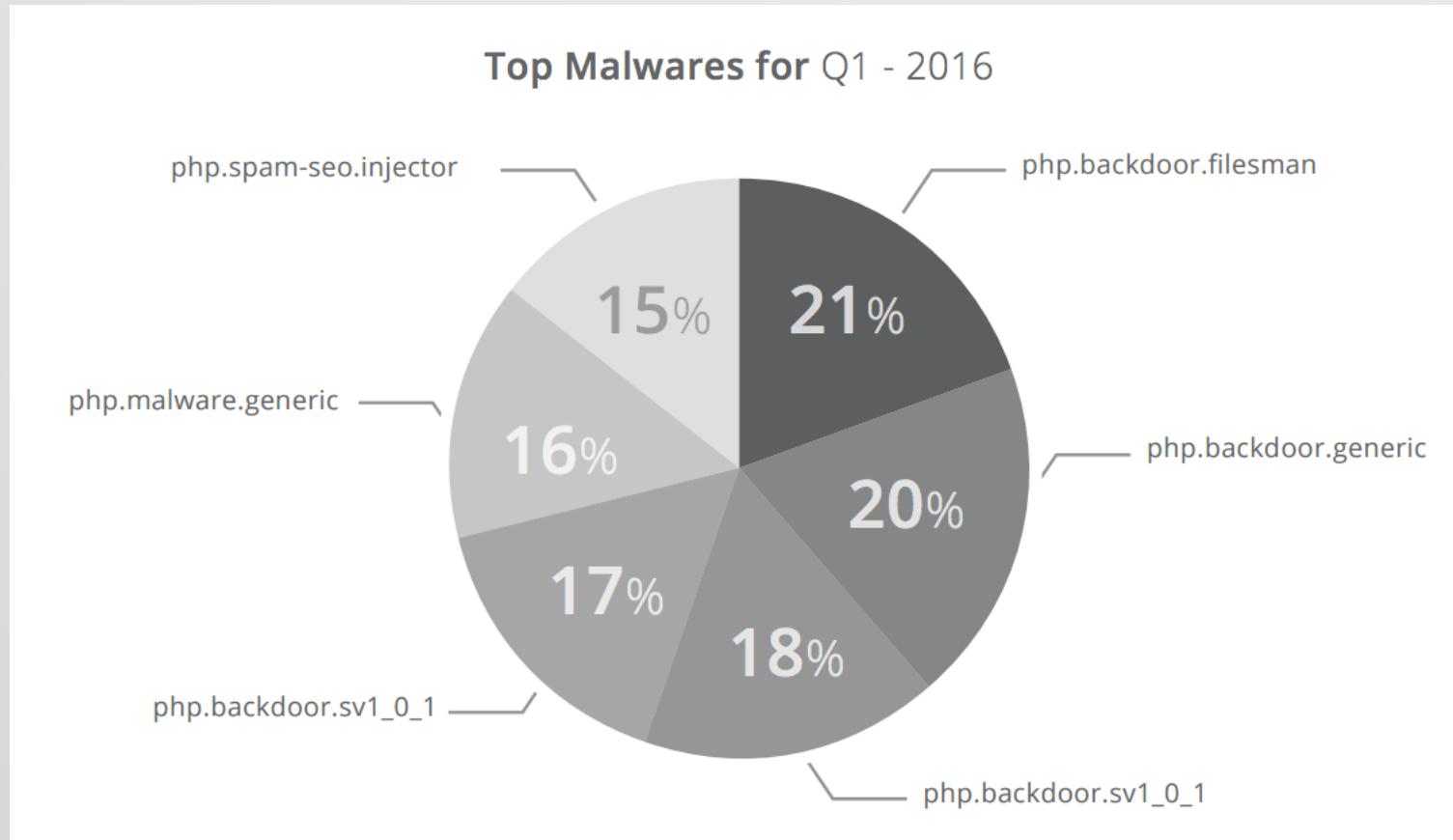


- RevSlider representa el 10% del total de las infecciones.
- El bug de TimThumb tiene 4 años de estar afectando sitios web.
- El problema de RevSlider es que viene incrustado en themes pagados.

Más estadísticas sobre infecciones



Más estadísticas sobre infecciones



Tipos de Infección



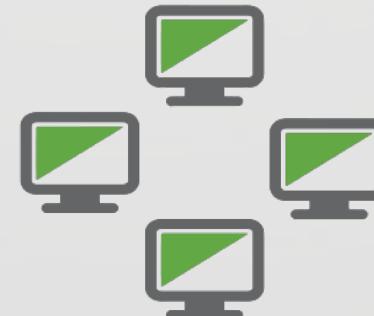
Malware



Envenamiento
de resultados
de búsqueda



Phishing



DDoS/Bots/Backdoors

Tipos de Infección

- Spam Email
- Defacement
- Ransomware

Los Impactos del compromiso de tu sitio web

COMERCIALES



Brand



Economic



Emotional Distress

TECNICOS



Website Blacklisting



SEO Impacts



Visitor Compromise

Un Ambiente Complejo



Computadora: Trojanos, keyloggers, computadora desenllavada, etc

LAN/WIF: Sniffers, traffic loggers, etc

User: Passwords inseguros, passwords en postips, agendas, etc.

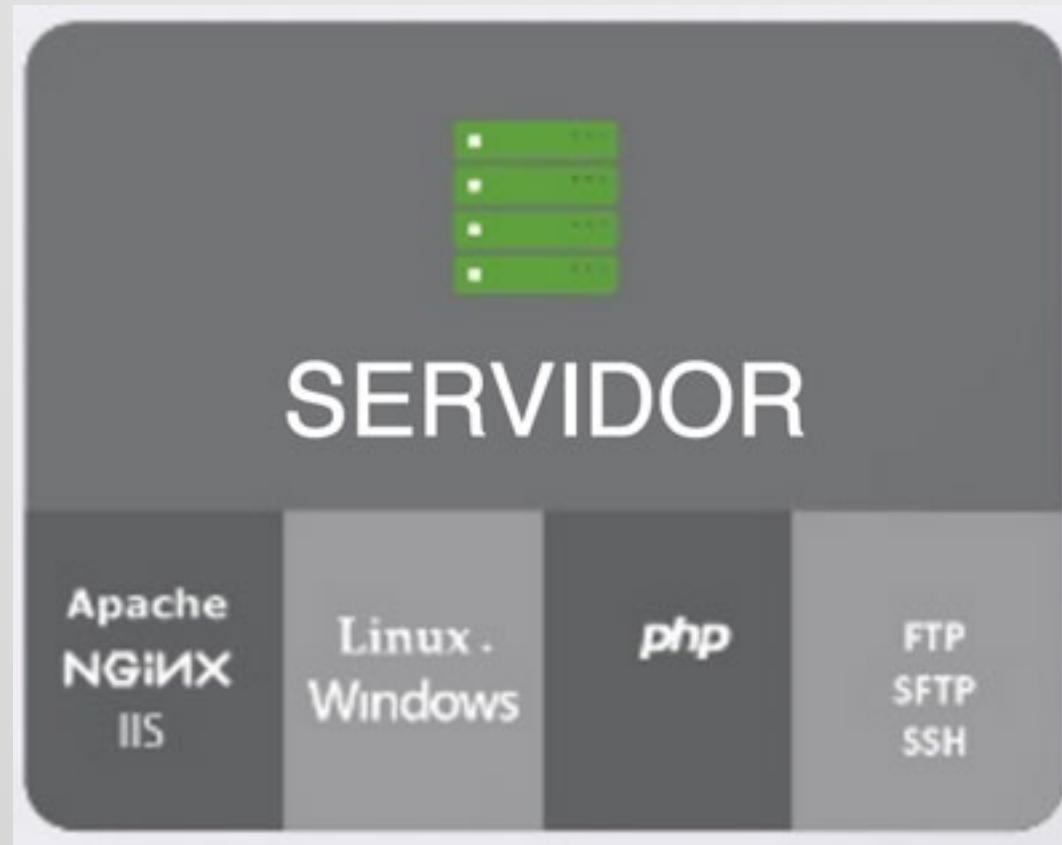
Un Ambiente Complejo



Wordpress: XSS, SQL Injections, fingerprinting

cPanel: bugs, cross site contamination, etc.

Un Ambiente Complejo



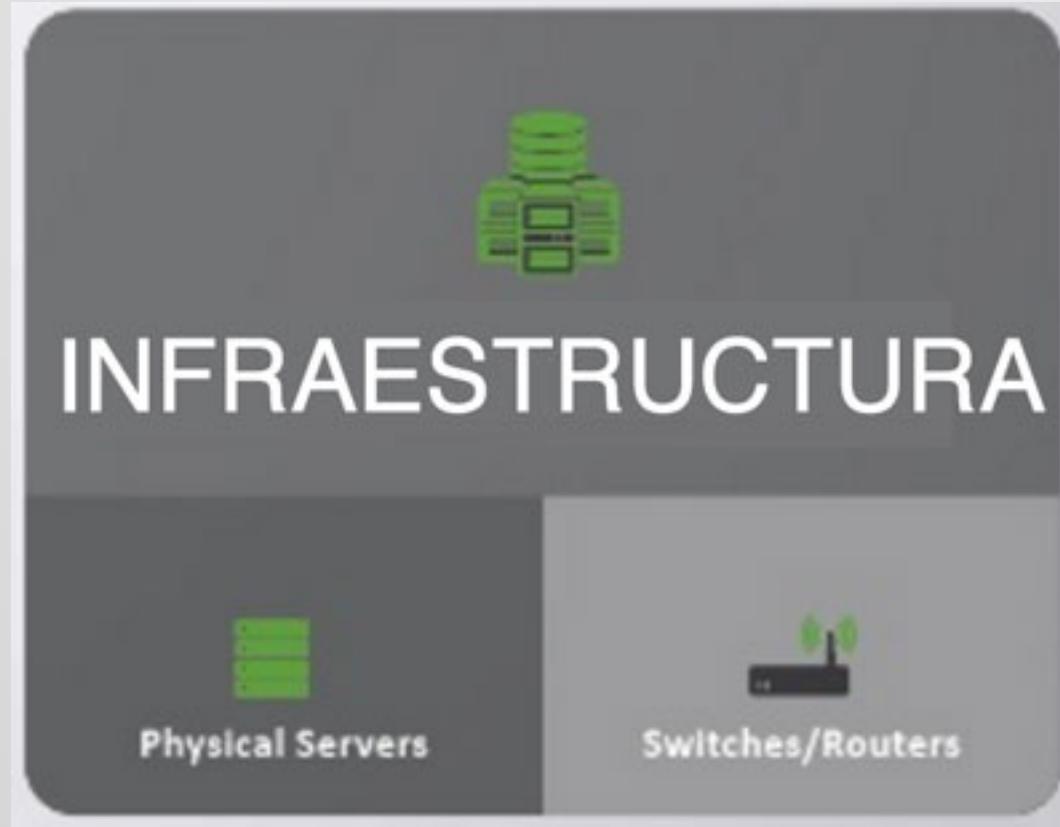
Linux: bugs en kernel. Fingerprinting, password debil root.

Librerias: bus como Imagemagick, ssl, etc

Windows: bugs, fingerprinting.

PHP: bugs, write permissions. etc

Un Ambiente Complejo



Acceso a los servidores

Puertos USB

Port Hijacking, IP Hijacking etc.

Redes: Sniffing, DDoS

Un ambiente seguro

Tiene que tener políticas seguras en cada ambiente



O seremos víctimas de...



Tienen alguna pregunta hasta ahora?
(hora de tomar un poco agua)

NO? Ok sigamos...

Tipos de ataque

Ataques Dirigidos

- Ocurre 0.01% de las veces
- Hay un objetivo específico
- No se conoce la vulnerabilidad al inicio, sino que se define después de pruebas
- Automatizada o Manual
- Alto nivel de expertise o habilidades
- Motivos personales: políticos, rivales/competencia, odio, financieros.

Ataques Oportunistas

- Ocurre 99.99% de las veces
- No hay un objetivo específico
- Se ataca una vulnerabilidad específica conocida.
- Mayoritariamente automatizada
- Nivel bajo/intermedio de habilidades
- No es personal

Flujo del ataque



Flujo del ataque

FASE	ATAQUE DIRIGIDO	ATAQUE OPORTUNISTA
RECONOCIMIENTO	Explorar un ambiente específico	Explorar la web por un problema específico
IDENTIFICACION	Identificar los posibles vectores de ataque en la red	Ocurre en la fase de reconocimiento
EXPLOTACION DE VULNERABILIDAD	Explota vulnerabilidades basada en los servicios que contenga el ambiente	Explota vulnerabilidades conocidas
SUSTENTABILIDAD	Aseguramiento de que el atacante pueda seguir entrando al sistema	
COMPROMISO		Cumplir objetivo
LIMPIEZA	Reducir probabilidades de detección y borrar huellas	N/D

Flujo del ataque

FASE	CONSIDERACIONES	CONTROLES DE SEG.
RECONOCIMIENTO	¿Como estamos reduciendo la superficie de ataque?	Desactivar servicios/sitios web sin uso, puertos, aplicaciones.
IDENTIFICACION	¿Cómo sabemos que hay vulnerabilidades?	Administración de Vulnerabilidades (wpscan, sitecheck, etc)
EXPLOTACION DE VULNERABILIDAD	¿Cómo estamos mitigando los intentos de explotar vulnerabilidades?	Usar un WAF/IPS basado en la nube
SUSTENTABILIDAD	¿Cómo sabemos que no hay backdoors?	Usar sistemas IDS
COMPROMISO	¿Cómo sabemos que no estamos comprometidos?	Usar IDS para revisar integridad del sistema
LIMPIEZA	¿Estamos reteniendo las bitacoras remotamente y backups?	Revision de logs y realización de backups

¿Cómo son hackiados los sitios web?

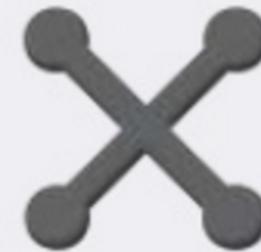
Control de Acceso



Vulnerabilidades
de Software



Contaminación
cruzada de sitios



Hosting



Integración con
aplicaciones de
3ros

Control de Acceso



- Se refiere al como se accesa a ciertas areas, lugares o cosas
- El control de Acceso a sitios web se extiende a todas las aplicaciones que brindan algún tipo de acceso al ambiente web
 - Panel de control del CMS (WP-ADMIN)
 - Panel control de hosting (cPanel, Plesk, Parallels, etc)
 - Nodos de acceso (SSH, sFTP, Email, etc)
- Cuando pensemos en control de acceso, pensemos mas allá del sitio web o ambiente aplicativo.
- Los ataques al Control de Acceso vienen en forma de ataques bruteforce.

Vulnerabilidades de Software



- Se refiere los bugs en el código de los aplicativos que pueden ser abusados. Incluyen cosas como:
 - Inyección SQL, Cross-Site Scripting (XSS), Remote Code Execution (RCE), Remote File Intrusion (RFI), etc.
- Los CMS luchan con las vulnerabilidades de sus extensiones: plugins, temas, modulos, componentes, etc.
- Sugerencia familiarizarse con los proyectos y suscribirse a alertas de seguridad.

Contaminación Cruzada de sitios web



- Se refiere al movimiento lateral de las infecciones una vez que entra a un servidor.
- Este es un ataque interno y no externo. El atacante entra al servidor a travez de un sitio vulnerable y luego lo usa como pie de amigo para infectar el resto de los sitios web en el servidor.
- Es la razón #1 para la reinfección de sitios web, los propietarios de sitios web se concentran en el sitio web afectado y los sintomas, pero no revisan los sitios web que no muestran señales externas o visibles de compromiso.
- Este método es super exitoso en los ambientes que no utilizan métodos funcionales de aislamiento en el servidor, o que usan los permisos o configuraciones incorrectas.

Integración con 3ros



- Se refiere un sin numero de cosas, pero últimamente lo más prevalente son los servicios de Anuncios (Ads) y sus networks de anuncios asociados.
- Estas integraciones introducen un eslabon debil en la cadena de seguridad. Estos Networks de Anuncios son atacados, infectados y utilizados para penetrar otros sitios web. **Malvertising**.
- Malvertising, es el acto de manipular los anuncios para distribuir malware, a menudo en la forma de redireccionamiento maligno y downloads no solicitados.
- Son extremadamente dificiles de detectar debido a su naturaleza condicional, y que están fuera del ambiente del sitio web.

Hosting

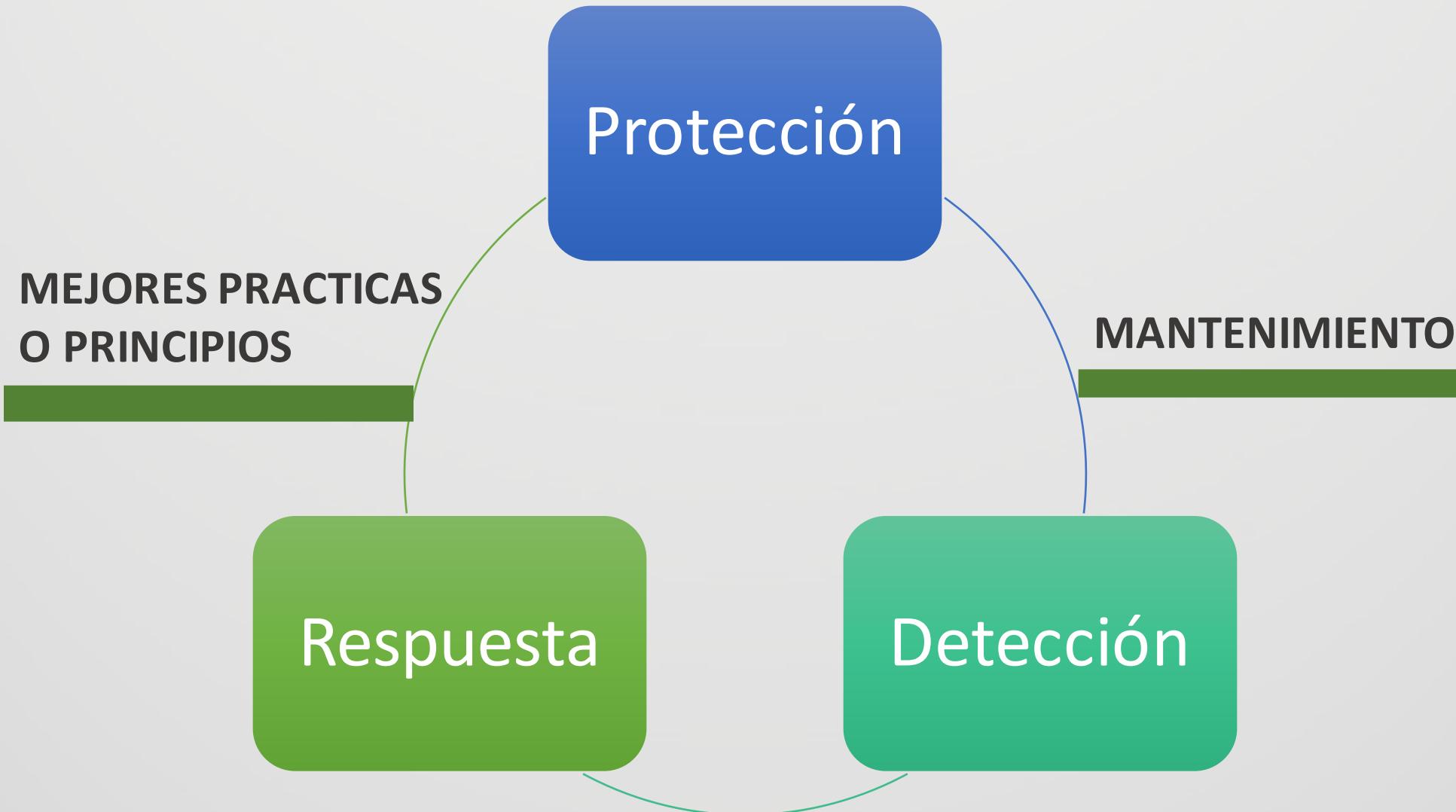


- Hace muchos años que no se ha dado un compromiso masivo de un proveedor de shared hosting grande. La última vez fue GoDaddy en 2011 (.htaccess redirect)
- El mayor problema en nuestros días, no son estos proveedores, sino organizaciones que intentan ofrecer una solución completa: Marketing, Desarrollo, Seguridad, Hosting, SEO, etc.
 - Proveedores con poca experiencia que introducen confusión y ruido un ecosistema de por si ya saturado.
 - Saben lo suficiente para ser peligrosos, pero les faltan habilidades y conocimiento
 - Contribuyen a un gran numero de contaminación cruzada debido a malas configuraciones.

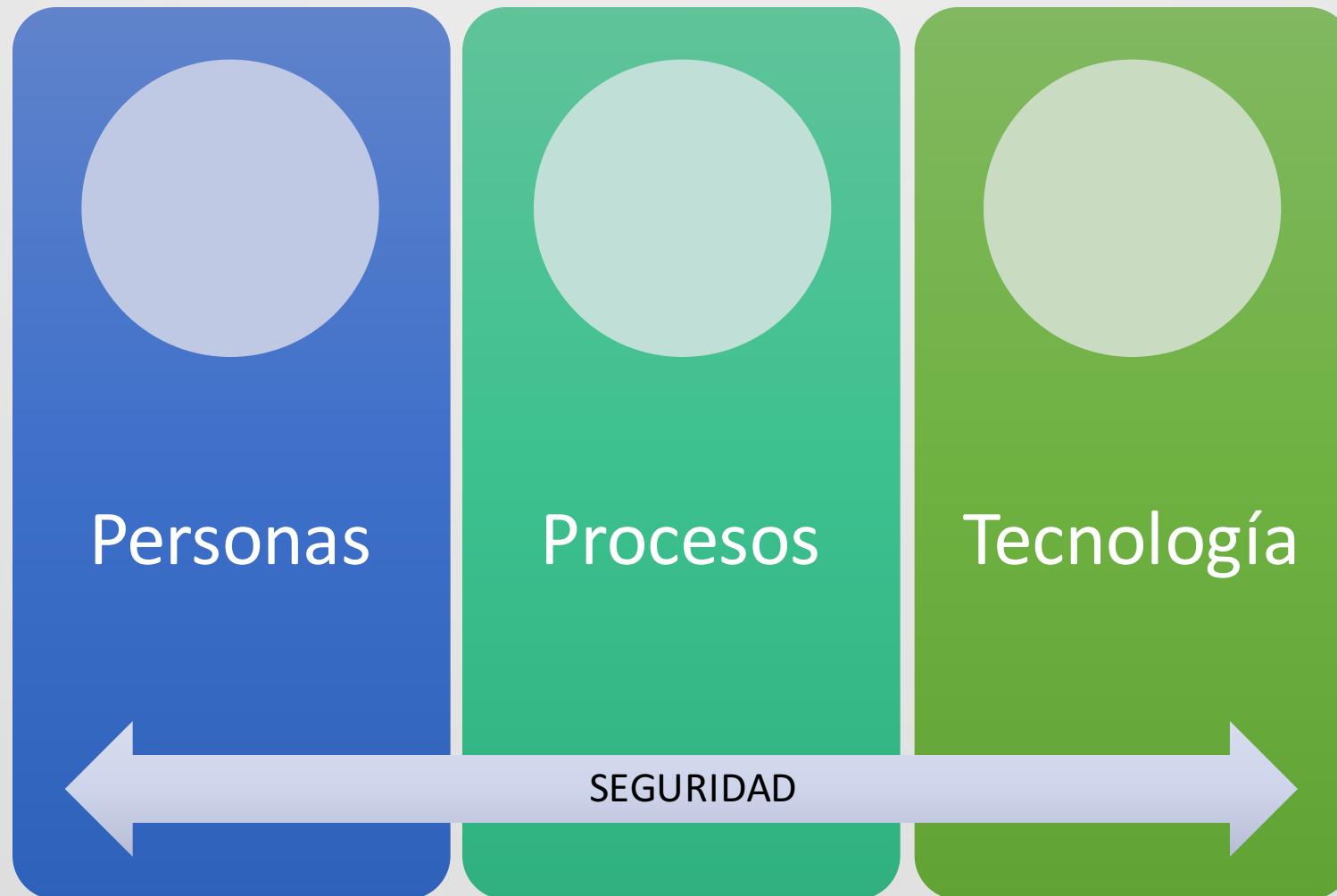
¿Pensando sobre seguridad?

Ideas sobre como mejorar tu postura sobre seguridad en sitios web

La SEGURIDAD no es un proceso estático,
Es un PROCESO CONTINUO



La tecnología **NUNCA REEMPLAZARA**
tu responsabilidad como dueño de un sitio web



La seguridad **NO ES** un Proyecto Hazlo Tu Mismo
(DIY – Do It Yourself)

DEFENSE IN DEPTH



A layered approach to proactive and reactive website security.



RESPONSE



Professional incident response team available 24/7/365.

PROTECTION



Website Application Firewall (WAF) & Intrusion Prevention System (IPS).

DETECTION



Continuous website security monitoring to quickly identify potential Indicators of Compromise (IoC).

P & R

Preguntas y Respuestas