Malware Moderno en la red Universitaria

Jesús Díaz
jdiaz@paloaltonetworks.com

RedIRIS 2011

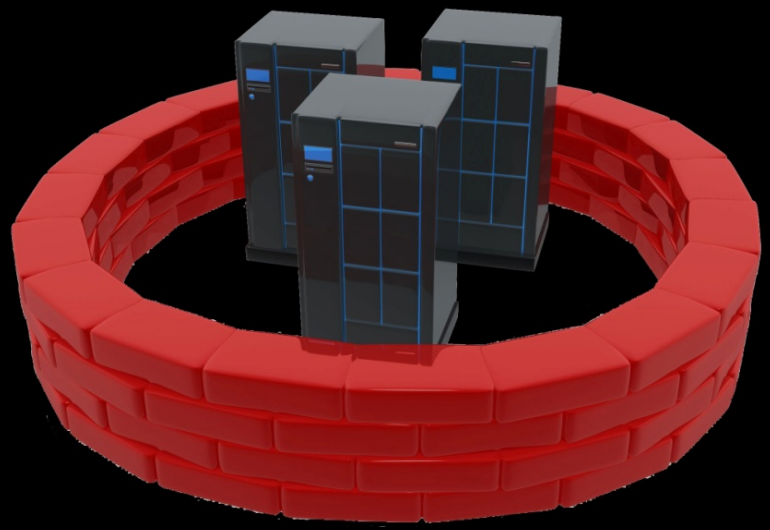
paloalto NETWORKS

the network security company™

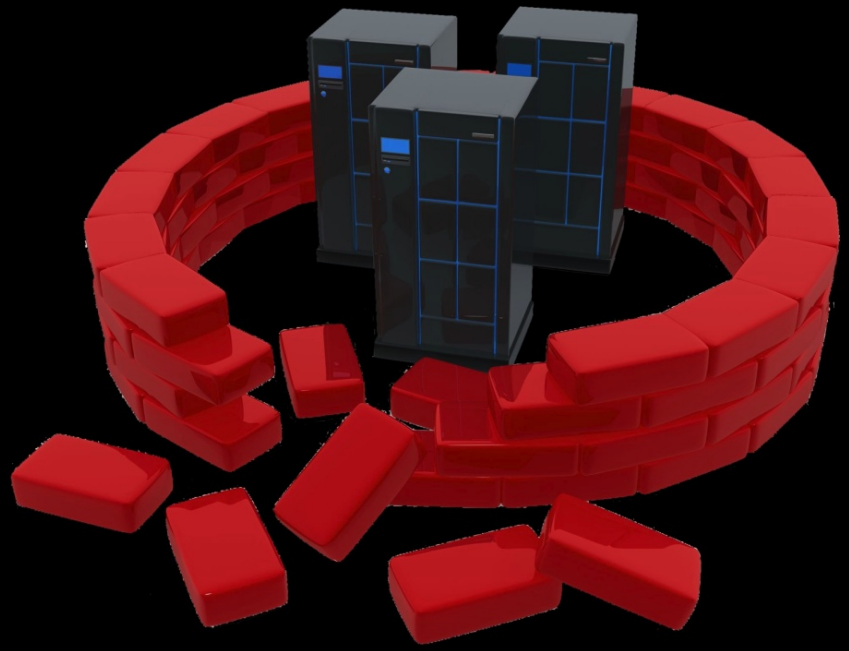

RSA
epsilon
PlayStation™

Mitología en las brechas de seguridad

Invertimos en proteger nuestros datacenters



En raras ocasiones el datacenter es atacado directamente



Ya no hay tanto escaneo de vulnerabilidades

El nuevo atacante

El nuevo atacante no es un “friki” aburrido

Se trata de naciones y crimen organizado, con objetivos económicos en muchos casos

Cómo funcionan las brechas de seguridad en 2011

Primer paso: crear un cebo atractivo para el usuario final

Primer paso: cebo para el usuario final

Lanzamiento del *phishing*

Primer paso: cebo para el usuario final

Segundo paso: se explota una vulnerabilidad

Tercer paso: se descarga una *backdoor*

Cuarto paso: se establece un canal trasero

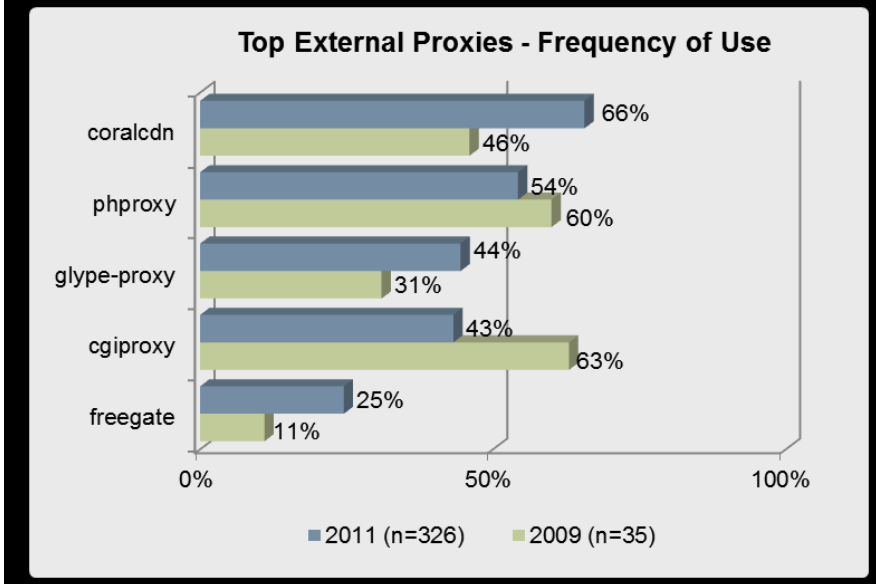
Quinto paso: explorar y robar

Análisis de la utilización de la red Universitaria y el malware

"Academic Freedom and Application Chaos" - Marzo 2011
http://www.paloaltonetworks.com/literature/higherEd_report.php

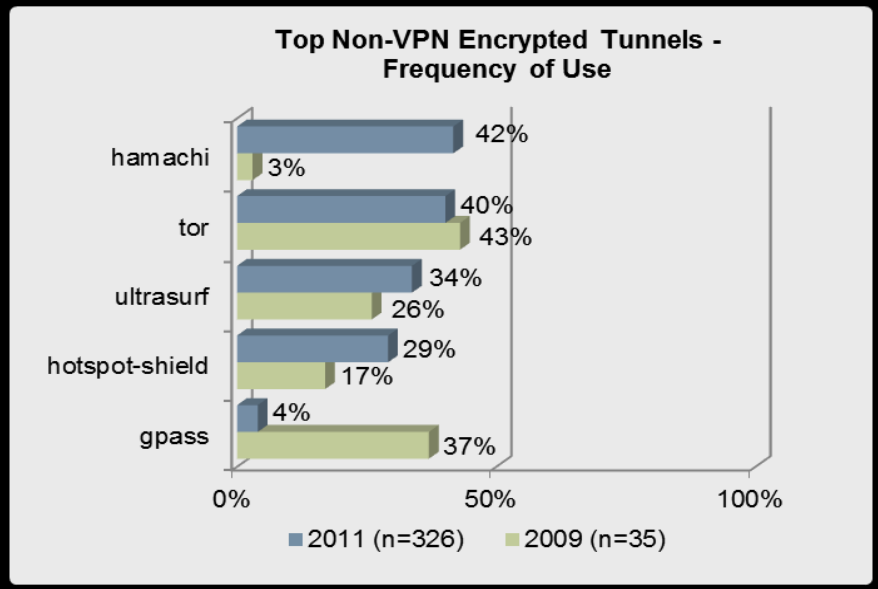

326
Universidades
64
PetaBytes
1.075
aplicaciones
Mucho en
común

Los estudiantes encontrarán el camino…

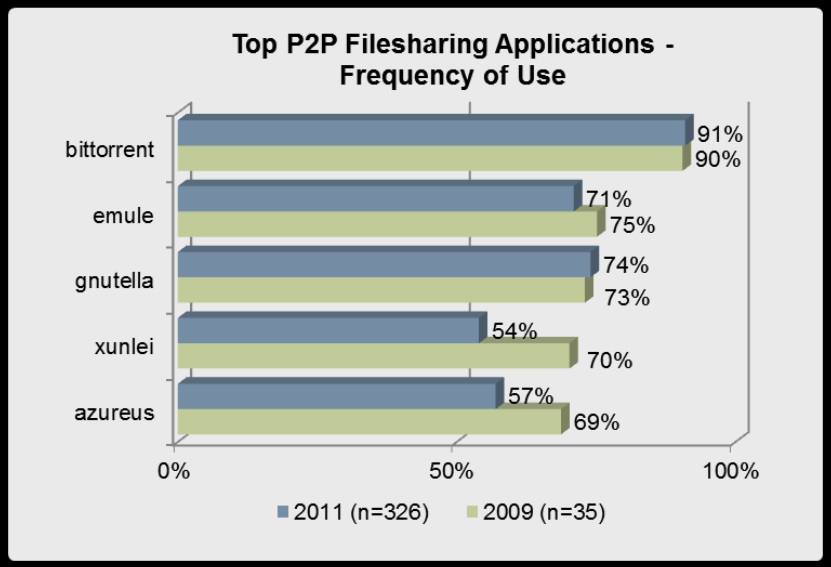


97% incidencia

65% incidencia

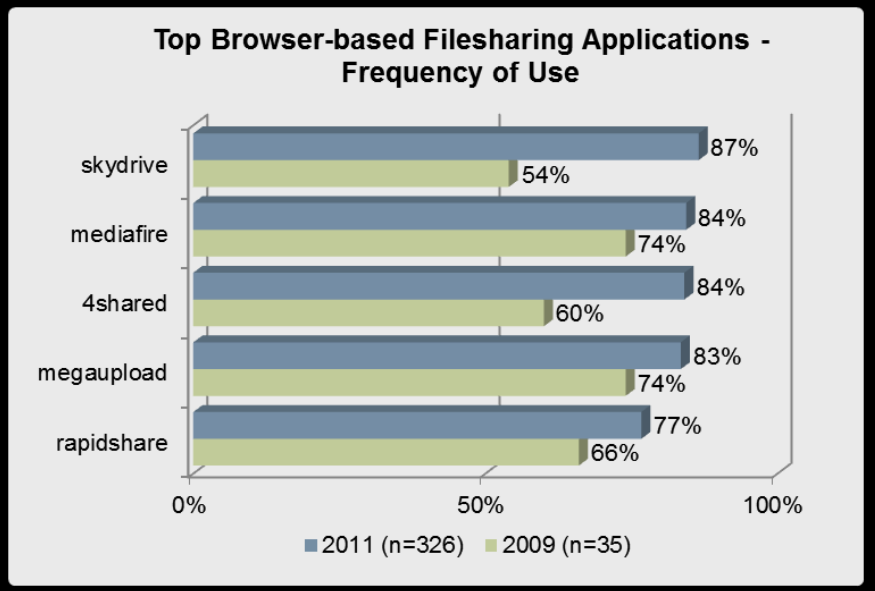


El uso de filesharing es abrumador

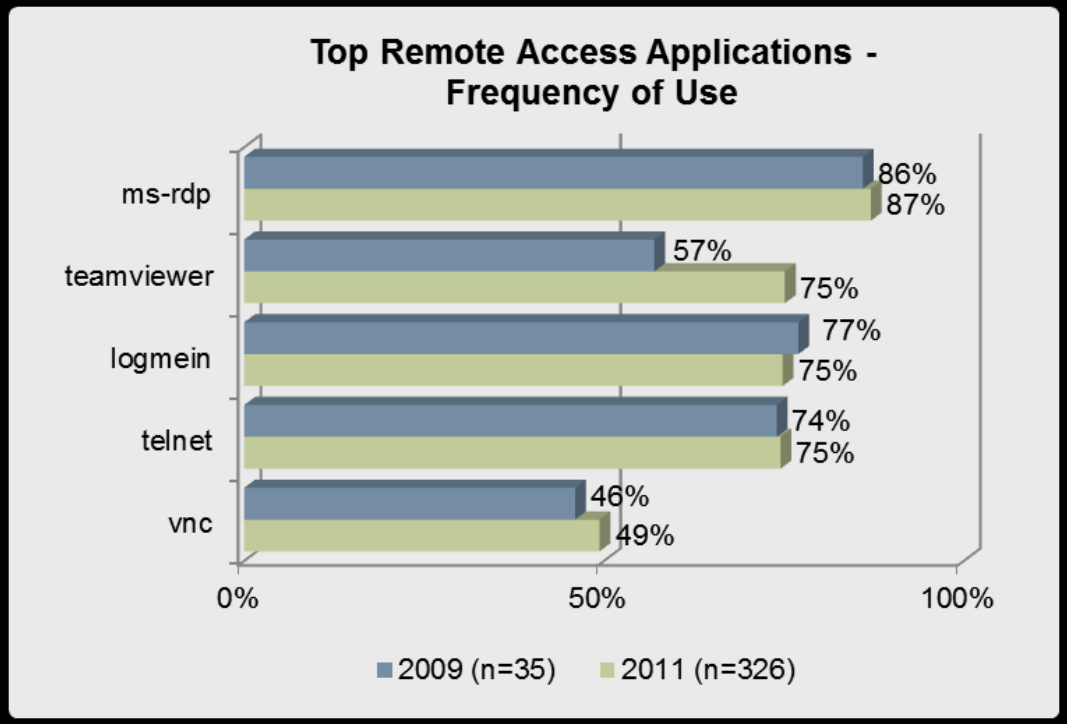


94% incidencia

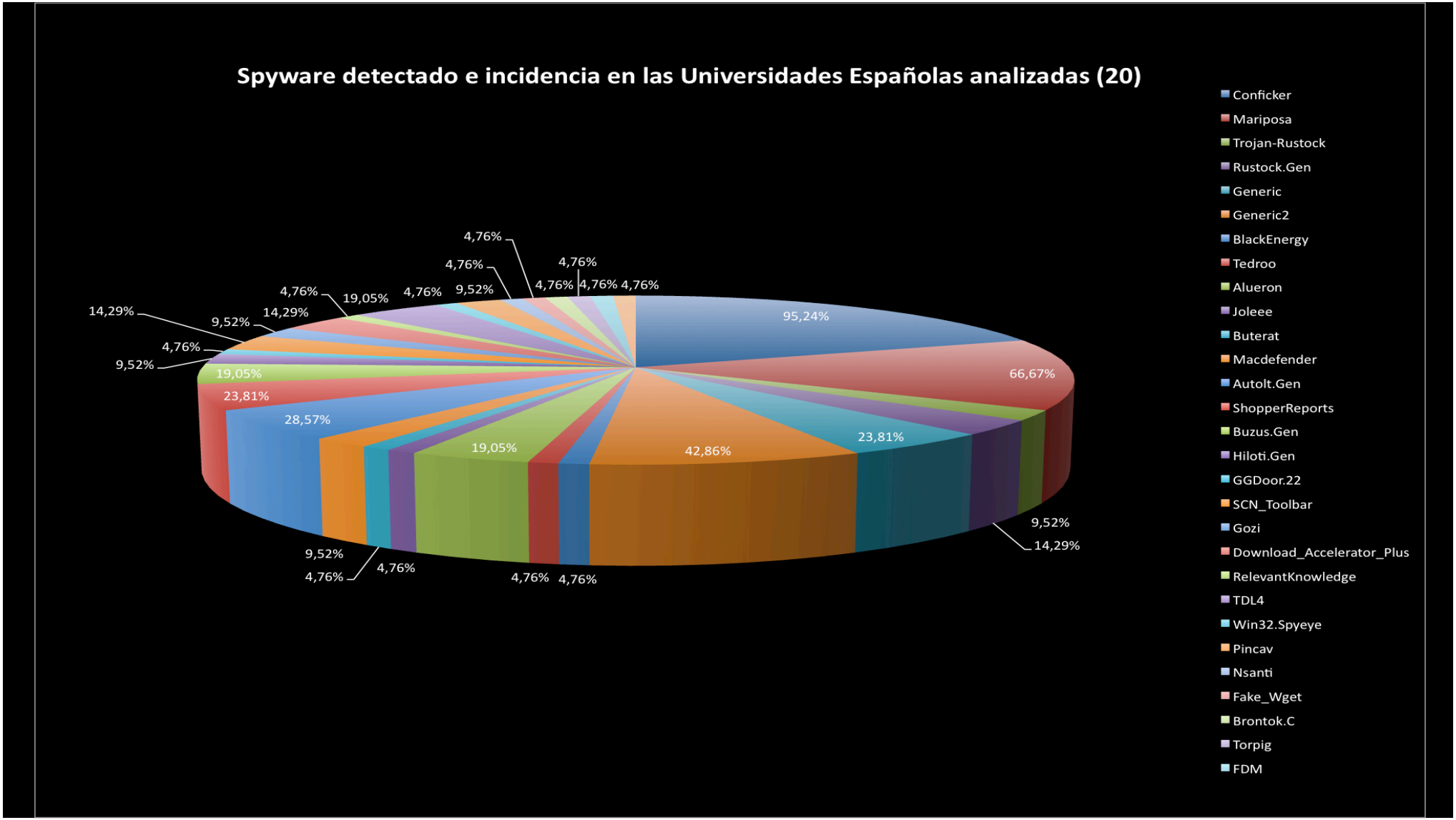
96% incidencia



El acceso remoto: ¿IT, soporte o estudiantes?



96% incidencia


Spyware detectado e incidencia en las Universidades Españolas analizadas (20)
95,24%
66,67%
42,86%
23,81%
19,05%
28,57%
23,81%
19,05%
14,29%
9,52%
14,29%
9,52%
4,76%
9,52%
4,76%
4,76%
4,76%
4,76%
4,76%
4,76%
4,76%
4,76%
4,76%
4,76%
4,76%
4,76%
Conficker
Mariposa
Trojan-Rustock
Rustock.Gen
Generic
Generic2
BlackEnergy
Tedroo
Alueron
Joleee
Buterat
Macdefender
Autolt.Gen
ShopperReports
Buzus.Gen
Hiloti.Gen
GGDoor.22
SCN_Toolbar
Gozi
Download_Accelerator_Plus
RelevantKnowledge
TDL4
Win32.Spyeye
Pincav
Nsanti
Fake_Wget
Brontok.C
Torpig
FDM

Deteniendo el malware moderno en práctica: WildFire

La protección es necesaria en todas las fases

Cebo

Exploit

Backdoor

Canal Trasero

Robo

Retos actuales

Los ficheros infectados están ocultos

- Dentro de las aplicaciones
- A través de tráfico cifrado, proxies
- Sobre puertos no estándar
- Drive-by-downloads

Incapacidad de reconocer ficheros con malware

- Malware focalizado
- Malware nuevo, desconocido
- Mucho tiempo hasta protección

Puntos de control no fiables

- Las sandboxes no son el punto de control, mientras que los puntos (fws) carecen de la inteligencia de la sandbox
- Falta de control para tráfico saliente

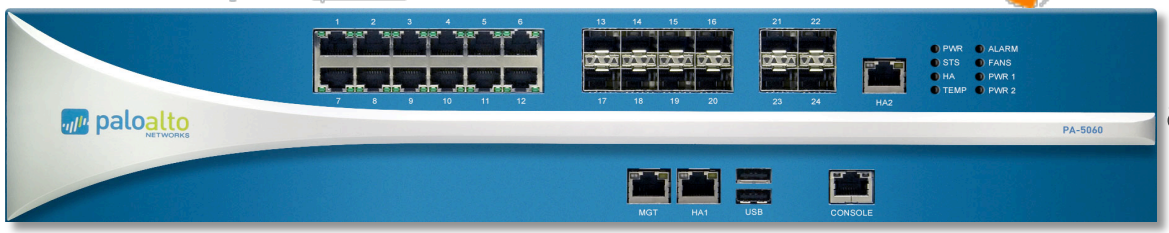
WildFire en acción

Ficheros desconocidos desde Internet

- Comparación fich. conocidos
- Entorno Sandbox
- Generador de Firmas
- Portal Web Administración

El Firewall sube el fichero a la nube WildFire

Las firmas se sirven a TODOS los Firewalls a través de updates regulares. El portal ofrece análisis forense.



WildFire en acción

- Identifica el malware desconocido a través de la observación directa, en una sandbox virtual en la nube
  - Detecta más de 70 comportamientos maliciosos
  - La captura y la protección la realiza el firewall
  - El análisis realizado en la nube elimina la necesidad de adquirir hardware nuevo y proporciona un punto central de visibilidad
- Automáticamente genera firmas para el malware identificado
  - Ficheros de infección y command-and-control
  - Distribuye las firmas a todos los firewalls a través de updates regulares
- Proporciona análisis forense sobre el comportamiento del malware
  - Acciones realizadas sobre la máquina objetivo
  - Aplicaciones, usuarios y URLs relacionadas con el malware

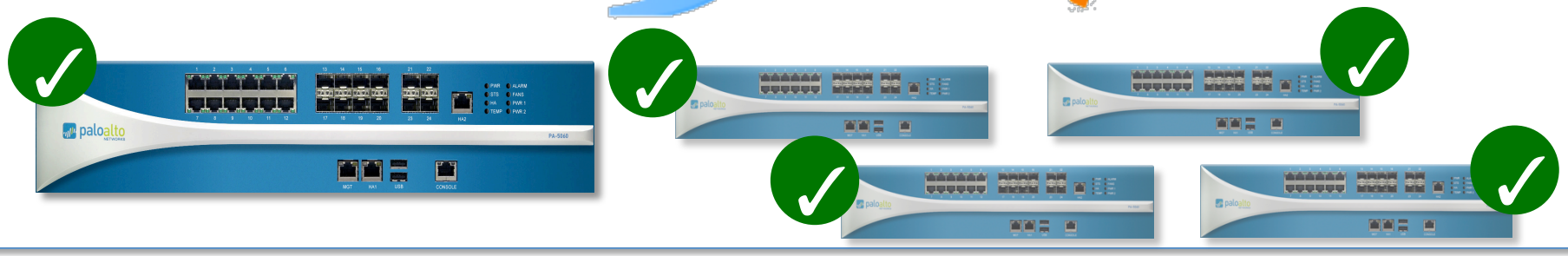
WildFire en acción

Es necesario un NGFW

- Debe decodificar las apps para buscar ficheros ocultos
- Debe controlar el SSL, y las tácticas evasivas
- Aplicación en línea y bloqueo del tráfico C&C

Análisis Centralizado

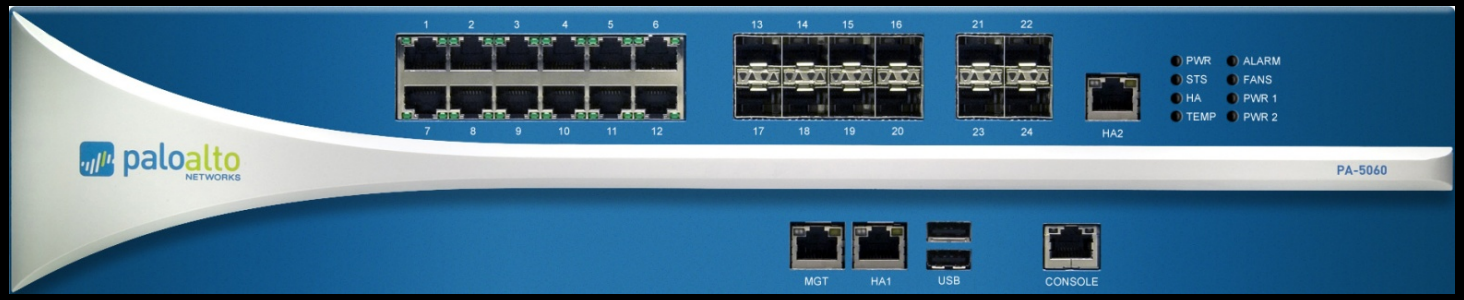
- Inteligencia y protección compartido con TODOS los firewalls
- Sin necesidad de reevaluar ficheros
- Actualizar fácilmente la lógica de detección
- Sin necesidad de utilizar nuevo hardware



Estadísticas WildFire durante la fase Beta

- WildFire recibió 35.387 muestras y más del 7% fue clasificado como malware (unas 2.500)
- De este malware, el 57% no tenía cobertura por ningún fabricante de AV, ni había sido visto por Virus Total en el momento del descubrimiento (unos 1.400)
- Hotfile y AIM-Mail tuvieron una actividad malware muy alta, con un ratio de ficheros infectados de 10:1 frente a los limpios
- El 15% del malware nuevo generó tráfico desconocido

Conclusión: la protección frente al malware avanzado es tarea de un *next generation firewall*



Vídeo de demo

¡Gracias por su atención!

Jesús Díaz
jdiaz@paloaltonetworks.com

RedIRIS 2011

paloalto NETWORKS

the network security company™