

- Seguridad en los datacenters



OWASP

The Open Web Application Security Project

About Me



OWASP

The Open Web Application Security Project

- By alpha_one_x86 (BRULE Herman)
- alpha_one_x86@first-world.info
- Sys admin en e-commerce
- Tech y innovacion
- Author de Supercopier/Ultracopier (Botnet de 2 millones de bot), CatchChallenger (MMORPG y cluster multired)



DDOS

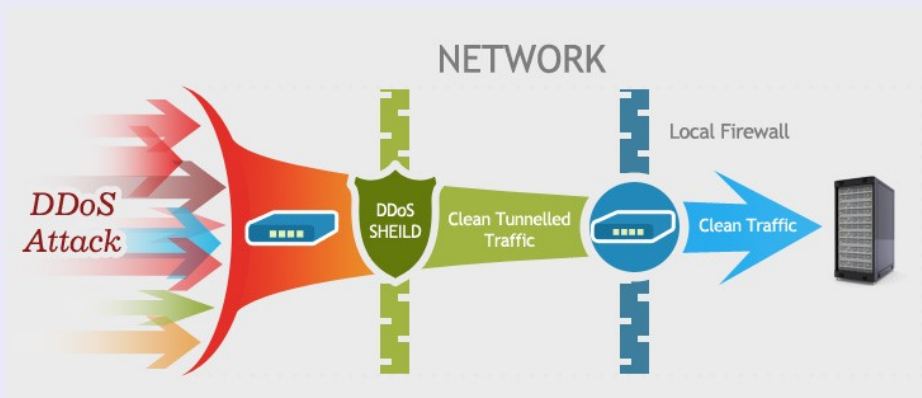


OWASP

The Open Web Application Security Project

Un ataque de denegación de servicios, es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema de la víctima.

Wikipedia



El atacado y el ataque



OWASP

The Open Web Application Security Project

El atacado esta definido por:

Carga característica (volumen como contenido del trafico)

Servidor simple o multiple

Punto fuerte o débil

Recursos (cpu, memoria, red)

El ataque es definido por:

Nivel OSI atacado

Carga (red, cantidad de botnet e ip, contenido)

Objetivo: apagar el servicio, desviar la atención

Filtro DDOS



OWASP

The Open Web Application Security Project

¿Filtrar sobre cual criterio (OSI 5+)?

Si hay mucho mensajes/peticiones al segundo de un cliente

Si en tiempo normal los clientes hacen: archivo 1, archivo A, archivo B, un cliente que solo carga el archivo 1 en tiempo de sobre carga es probablemente un bot

Grey list: si el trafico es nacional, si de golpe un país se conecta es sospechoso (falso positivo: buzz, media)

En la primera conexión es imposible o muy difícil de diferenciar un bot de un visitante normal (sin perfil)

Un filtro anti-DDOS divide el ataque (ex: 1% pasa), no lo anula.

Si hay varios filtros DDOS (principalmente varios servidores), la sincronización de la lista negra consume mas recurso pero aumenta la efectividad

El rendimiento



OWASP

The Open Web Application Security Project

Si el rendimiento es bajo, solo algunas ip son suficientes para saturar el servidor

Es muy difícil para los filtros DDOS eliminar el ataque porque no son ip que hacen peticiones rápidas, pero simplemente un visitante mas que navegue a un ritmo normal (es suficiente para saturar el servidor)

Si los 1% que dejar pasar el filtro anti-DDOS cae el sitio no se puede hacer nada

Bonus: Mas rendimiento = mejor resistencia a los DDOS y menos costo de infraestructura

Fuga de memoria/recurso



OWASP

The Open Web Application Security Project

La fuga de memoria hace que el servidor se sobrecargue solo con el tiempo, el ataque solo acelera el proceso

Valido para otros tipos de recursos: cache HDD que llena el disco poco a poco

Solución:

Purga automática

Verificar la fuga a la concepción y después de un tiempo de producción

Reinicio automático en caso de kill por el OS y limite del proceso estricto para matarlo cuando sobre pase sus limites

El botnet



OWASP

The Open Web Application Security Project

 **NORSE**

ATTACK ORIGINS

#	Country
2146	 China
1512	 United States
540	 Germany
445	 Netherlands
383	 Mil/Gov
317	 Russia
159	 Taiwan
146	 South Korea
133	 Hong Kong
81	 Thailand

ATTACKS

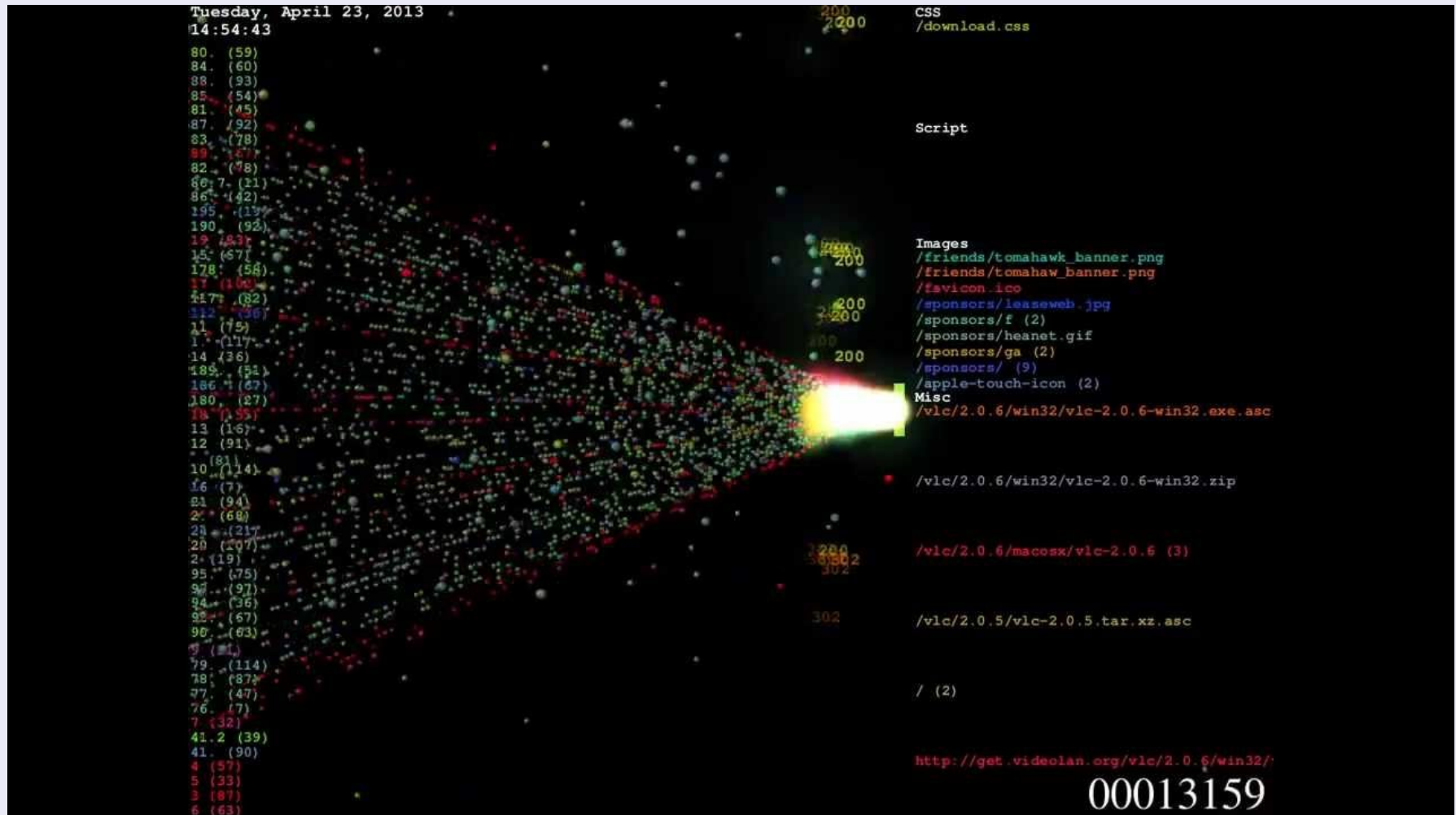
Timestamp	Organization	Attacker		Target		Type	
		Location	IP	Location	Service	Port	
2014-06-19 22:16:36.29	Webhosting.Net	Miami, United States	67.215.180.162	Miami, United States	unknown	22936	
2014-06-19 22:16:36.31	Taipei Taiwan	Taipei, Taiwan	111.240.227.163	Saint Louis, United States	isakmp	500	
2014-06-19 22:16:37.11	SingleHop	Chicago, United States	198.20.69.74	Seattle, United States	unknown	6379	
2014-06-19 22:16:37.25	Taipei Taiwan	Taipei, Taiwan	111.240.227.163	Saint Louis, United States	isakmp	500	
2014-06-19 22:16:37.26	Dowco Computer Systems	Burnaby, Canada	209.87.141.64	Mountain View, United States	microsoft-ds	445	
2014-06-19 22:16:38.16	Korea Telecom	Seongnam, South Korea	218.150.129.44	San Rafael, United States	telnet	23	
2014-06-19 22:16:38.17	CHINANET-HN Hengyang	Changsha, China	218.77.79.43	Saint Louis, United States	http	80	
2014-06-19 22:16:38.18	Taipei Taiwan	Taipei, Taiwan	111.240.227.163	Saint Louis, United States	isakmp	500	

El objetivo



OWASP

The Open Web Application Security Project

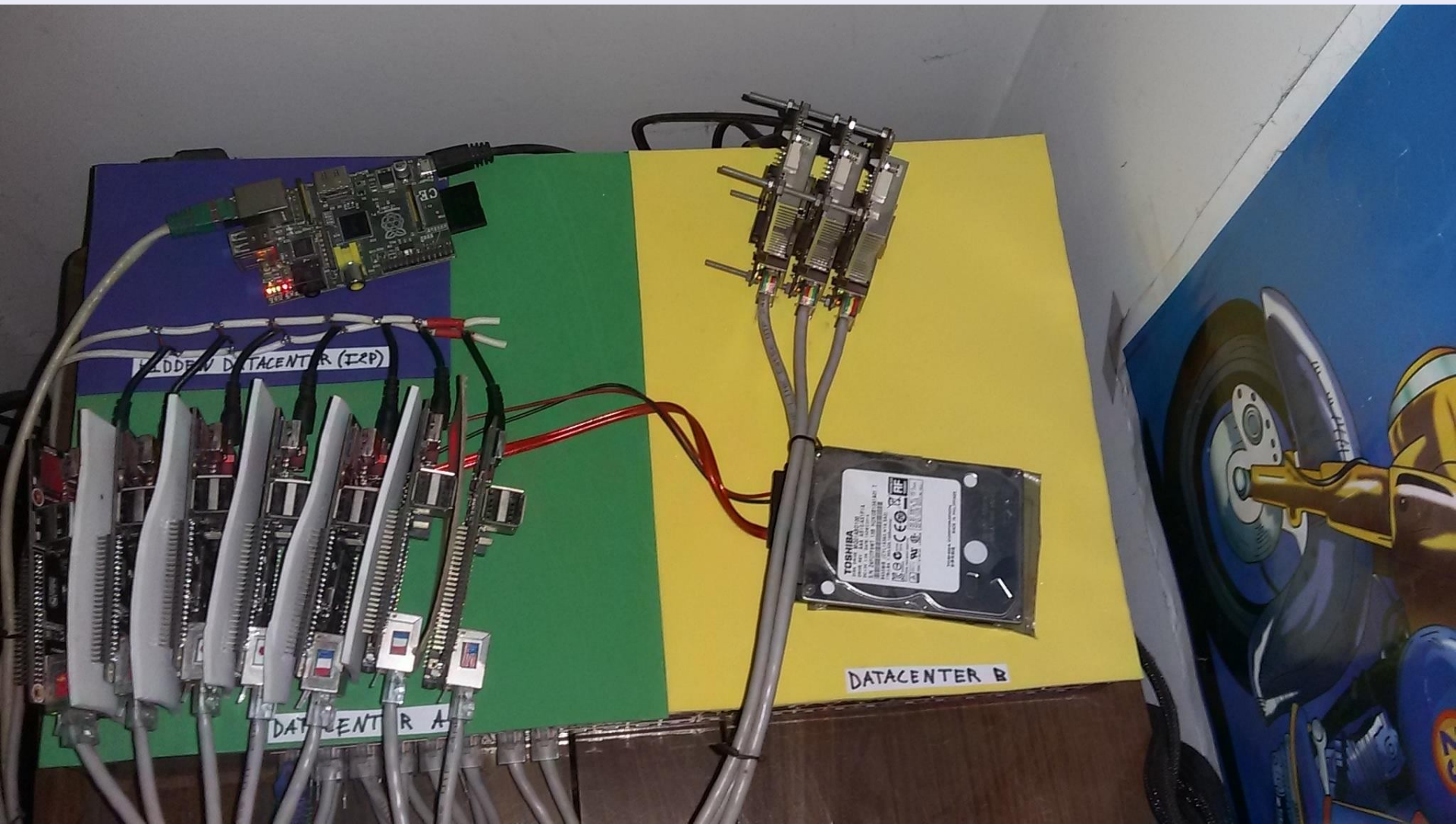


Portable datacenter



OWASP

The Open Web Application Security Project





Monitoreo del ancho de banda (OSI3-)

Limitation de los ataques internos

MAC/Ip spoofing

Protection de los routeur y web interface

Distribution segura y limpiar el HDD