Reporte de Poc CloudWAF

Elaborado por especialistas en seguridad

Julio 2020

Tabla de contenido

01 Objetivo..... 3
02 El Servicio CloudWAF..... 3
03 Generalidades de la Prueba..... 4
04 OWASP Top 10 Mapping..... 5
05 Conclusiones y Sugerencias.....8

01 Objetivo

Mostrar un informe que detalle los eventos aplicativos detectados en el período de duración de la prueba de concepto, y brindar al cliente un análisis de su situación actual de seguridad.

02 El servicio CloudWAF

El Servicio WAF en la Nube de Radware está basado en el firewall para aplicaciones web (WAF) líder en el mercado de Radware, que está certificado por ICSA Labs y ofrece cobertura completa contra los 10 principales ataques según el OWASP. Este servicio implementa simultáneamente los modelos de seguridad negativa y positiva, gracias a su capacidad única de adaptarse automáticamente a los cambios constantes en el panorama de amenazas y en los activos en línea que se deben defender.

El Servicio WAF en la Nube de Radware, creado con tecnologías de aprendizaje automático de última generación, detecta automáticamente los dominios de las aplicaciones, analiza las vulnerabilidades potenciales y asigna las políticas de protección óptimas. Este servicio controla y analiza continuamente los patrones de uso de las aplicaciones, y genera referencias granulares para el tráfico legítimo. Esto permite detectar y mitigar rápidamente los ataques de día cero, así como ajustar continuamente las políticas de seguridad ante cambios en los patrones de uso de las aplicaciones.

La tecnología de huellas digitales de dispositivos permite un seguimiento automático e independiente de la IP de aquellas fuentes maliciosas que intentan ocultarse detrás de cambios dinámicos de IP. Los activos web se mantienen protegidos en todo momento, incluso si las aplicaciones cambian constantemente y las amenazas evolucionan rápidamente. De esta manera, la seguridad está preparada para el futuro.

El Servicio WAF en la nube de Radware, que se activa con un simple cambio de DNS y no requiere hardware ni software adicionales, se puede implementar fácil y rápidamente para brindar seguridad web con un tiempo de implementación mínimo. El portal del servicio ofrece una facilidad de uso inigualable y visibilidad detallada de las alertas de ataque en tiempo real, así como estadísticas para permitir la planificación futura. Alertas de ataque en tiempo real brindan información sobre los ataques, los activos en riesgo y cómo responde el Servicio WAF en la nube. El Equipo de Respuesta a Emergencias de Radware, un grupo de expertos en seguridad web, ofrece asistencia adicional para la mitigación de ataques, los análisis forenses y la planificación futura.

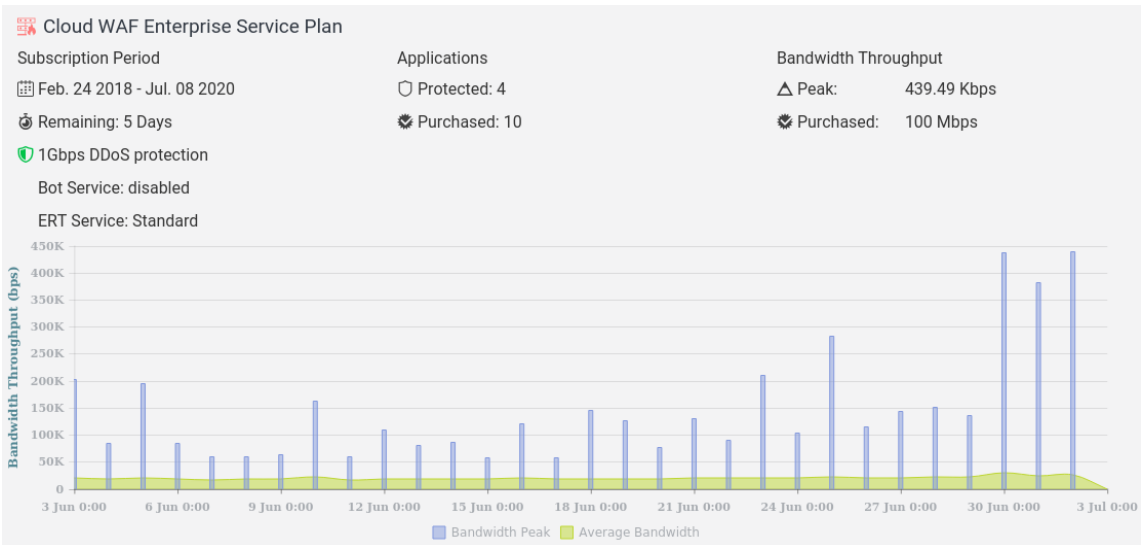
03 Generalidades de la prueba

- Se ofreció demostrar los beneficios de la solución de CloudWAF mediante una prueba de concepto funcional. En esta prueba de concepto se está protegiendo un portal de la elección del cliente, al cual pasamos a través de nuestras herramientas de seguridad WAF.
- La prueba demo comprendió un período de 30 días. Período en el que se realizó aprendizaje y afinamiento de las políticas de seguridad.
- El proceso comienza mediante la invitación por correo a una prueba de concepto. Este correo contiene una liga para generar una cuenta sobre el portal de CloudWAF de Radware y realizar el aprovisionamiento de aplicaciones. Durante el proceso de PoC, se permite la protección de 1 aplicación durante un período de 3 a 4 semanas. El portal seleccionado fue: *https://www.tuempresa.com/*

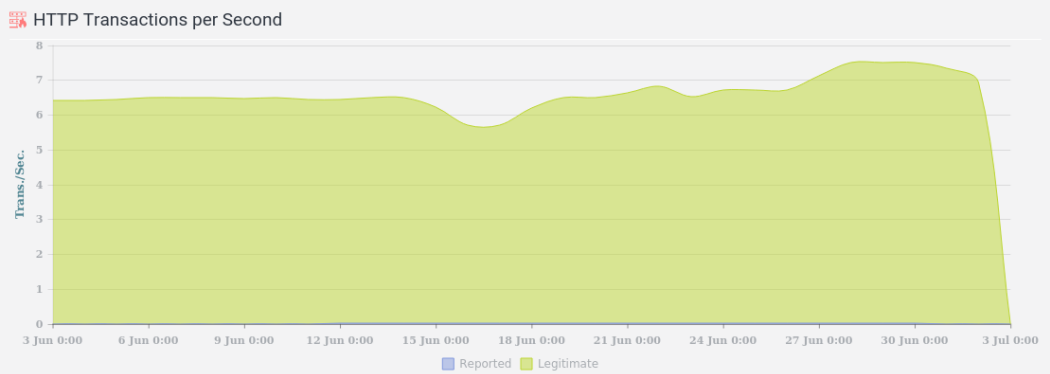
Inicialmente la prueba comienza en modo **Provisioning**. En este estado, se realiza toda la configuración inicial y aprovisionamiento para dar de alta el servicio. Este estado dura solamente unos cuantos minutos ya que el proceso es completamente automatizado.

Unos minutos después, la aplicación está en modo **Learning**, donde se redireccionó el tráfico del sitio web mediante la modificación de registros de DNS. A partir de esta etapa se comenzó a inspeccionar el tráfico y se presenta información estadística eventos en la aplicación.

Finalmente, después de un período de aprendizaje exitoso, 15 días después se modificó la aplicación para que funcione en modo **Protecting**. A partir de este momento, se detiene el paso de tráfico malicioso sobre el portal y solamente se permiten las transacciones legítimas.

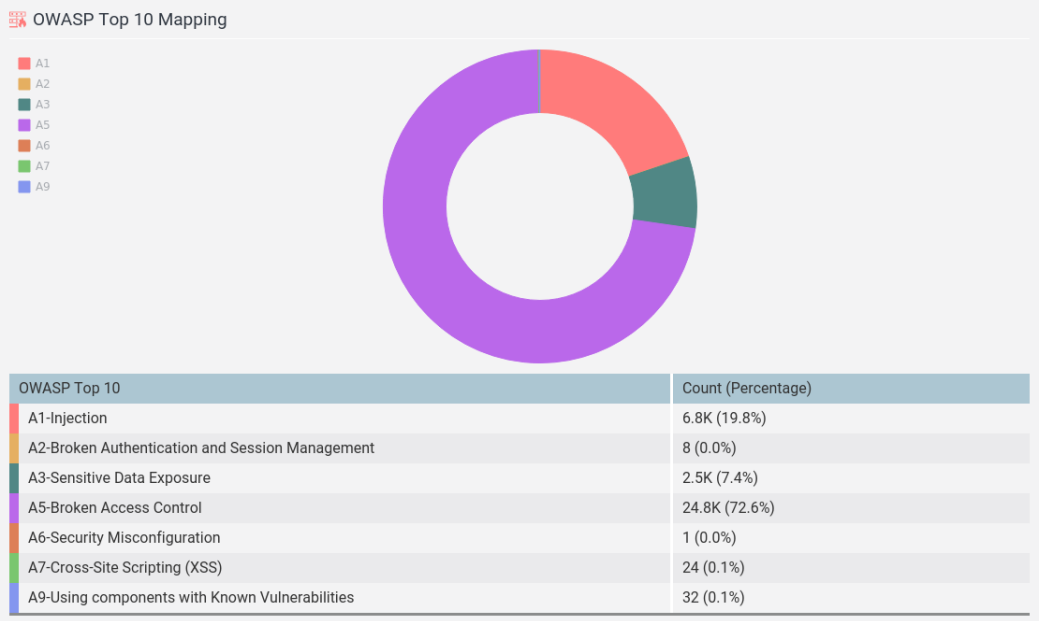


- Finalicemos esta sección mencionando que la aplicación tiene una tasa de peticiones alrededor de las 6 peticiones por segundo (en promedio), y notemos también que la tasa incrementa de manera proporcional al consumo de tráfico. Asimismo, la composición del tráfico es en su mayoría tráfico legítimo; aunque vimos miles de eventos, como mostraremos a continuación.



	Total (Transactions)	Percentage
Legitimate	17.1M	100%
Reported	3.9K	0%
Blocked	0	0%
Total	17.1M	100%

04 OWASP Top 10 Mapping



OWASP Top 10	Count (Percentage)
A1-Injection	6.8K (19.8%)
A2-Broken Authentication and Session Management	8 (0.0%)
A3-Sensitive Data Exposure	2.5K (7.4%)
A5-Broken Access Control	24.8K (72.6%)
A6-Security Misconfiguration	1 (0.0%)
A7-Cross-Site Scripting (XSS)	24 (0.1%)
A9-Using components with Known Vulnerabilities	32 (0.1%)

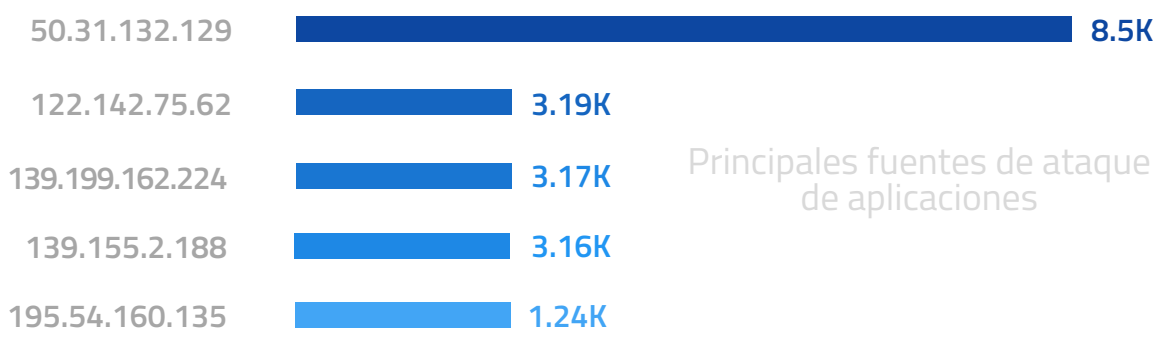
- Dentro de la categorización de OWASP Top-10 2017, las vulnerabilidades más comunes en las que incurre el portal son:

1.- A1:2017-Injection **19.8% de los eventos (6800)**: Dentro de esta categoría se engloban las vulnerabilidades que permiten la inyección de código en herramientas como SQL, NoSQL, OS o LDAP, lo que permite a los servidores interpretar una cadena como si fuese código, pudiendo acceder a la base de datos sin autorización.

2.- A5:2017-Broken Access Control **72.6% de los eventos (24800):** Errores en la configuración de los sistemas de control de acceso puede permitir a un atacante acceder a recursos y archivos para los que no debería tener permiso.

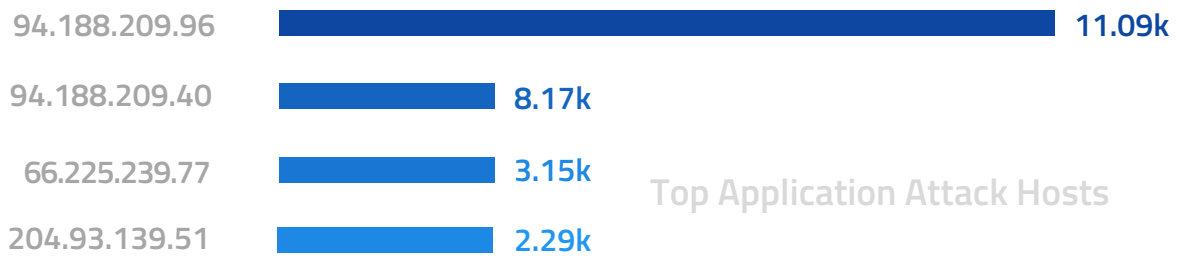
3.- A3:2017-Sensitive Data Exposure **7.4% de los eventos (2500):** Muchas aplicaciones web y APIs no protegen información sensible. Los atacantes pueden robar o modificar esa información débilmente protegida para llevar a cabo fraude, robo de identidad u otro tipo de crímenes. La información sensible puede ser comprometida sin protección extra tal como encriptación cuando la información está en tránsito o al almacenarse, y requiere precauciones especiales cuando se intercambia con el navegador.

- Principales IP´s que atacan la aplicación:



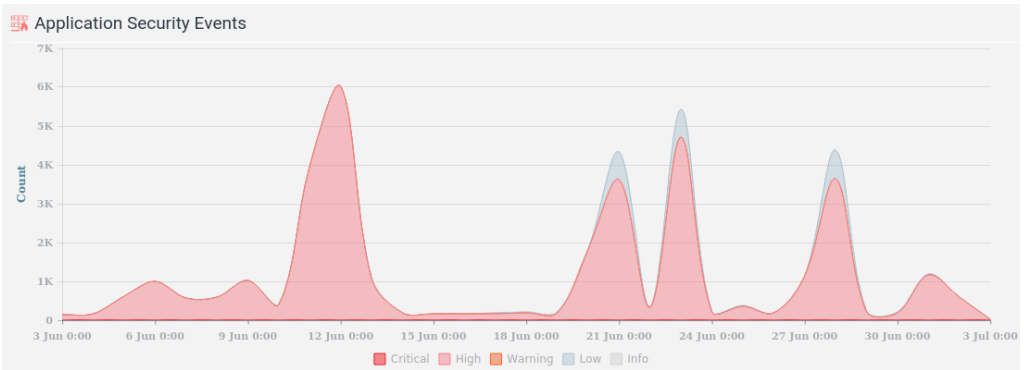
- Aunque la **IP 50.31.132.129** con **8.5k** eventos pertenece a Estados Unidos, el resto de las IP's pertenece a China y Rusia.

- Principales IP´s que atacan a los host:



- Aunque la **IP 94.188.209.96** con **11.09k** eventos pertenece a Israel, el resto de las IP's pertenece a Estados Unidos.

- En el primer día de implementación es cuando hemos tenido la mayor cantidad de eventos reportados, con cerca de **6 mil eventos** en el día. A pesar de esto vemos una distribución más bien constante de eventos rondando en un promedio de **3500** al día:



Severity	Daily Average	Daily Peak
Critical	0	0
High	1,149	6,004
Warning	0	0
Low	81	725
Info	0	0
Total Count	1,230	6,729

Con 1 mes de prueba es muy pronto para asumir; sin embargo, podemos preliminarmente notar una ligera tendencia hacia la baja en los eventos promedio por día. Esto es típicamente el resultado de que los ataques dejan de ser exitosos y los atacantes mueven sus herramientas a otros sitios más vulnerables.

05 Conclusiones y Sugerencias

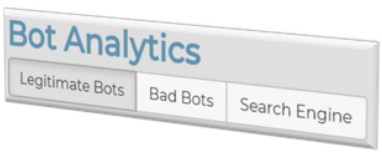
Durante la prueba se pudo observar que la aplicación no se encuentra libre de ataques. Existe un volumen considerable de eventos de seguridad que se ocasionan de forma constante. Este hecho nos permite concluir que una herramienta de protección de los portales es necesaria para evitar que este tipo de eventos maliciosos puedan llegar a afectar el portal. Recordemos que los hackers solamente necesitan que uno de los eventos sea exitoso para poder causar daños, y en el transcurso de la prueba se pudieron observar miles de intentos.

Los resultados también nos brindaron estadísticas interesantes del comportamiento de la aplicación. Información que deberíamos compartir con el equipo de desarrollo para facilitarles el trabajo de despliegue seguro de las aplicaciones, y una corrección de las vulnerabilidades de seguridad de raíz en caso de haberlas. Mientras tanto apoyarnos en las tecnologías de WAF para bloquear los eventos antes de que lleguen a afectarnos.

El servicio de CloudWAF de Radware es capaz de brindar esa capa de protección aplicativa que impide que los atacantes puedan vulnerar sus sitios web y al mismo tiempo, como pudieron evaluar, les brinda la información analítica para poder no solamente detener los ataques sino entender en tiempo real que es lo que está sucediendo con las aplicaciones.

El servicio incluye protección WAF basada en nuestra propia tecnología líder AppWall, e incluye también protección contra ataques de denegación de servicio basado en nuestra propia tecnología DefensePro, que es considerada la mejor tecnología para detener ataques de DDoS por múltiples firmas de analistas como IDC, Frost & Sullivan, Forrester, entre otros.

Para finalizar, mencionarles que nos encontramos listos también para brindarles estadísticas, análisis y protecciones relacionadas con el tráfico de Bots, ya que ahora también se encuentran disponibles los servicios de Bot Manager dentro del portal de CloudWAF, y que están basados en otra de nuestras tecnologías líderes de mercado: ShieldSquare.



Si necesitan conocer y clasificar el tráfico que proviene de Google, Bing y demás buscadores, al tiempo que eliminan el tráfico generado por bots maliciosos, podemos brindarles esta funcionalidad sobre sus aplicaciones protegidas sin necesidad de instalar o modificar su configuración actual.