INFORME

PRIORIZA LA SEGURIDAD DE TUS APPS

LAS AMENAZAS AVANZADAS CONTRA APLICACIONES REQUIEREN UN WAF AVANZADO

El panorama de amenazas es hoy muy distinto de como era hace 5 años. Los cortafuegos de aplicaciones web (WAF) de antes eran armas eficaces para mitigar los ataques a la capa de la aplicación, pero ahora tienen que enfrentarse al nuevo ritmo que marcan las capacidades avanzadas y la agilidad de los hackers. Las firmas suelen llegar después del ataque. Incluso aunque un WAF tradicional sea capaz de mitigar una amenaza, implementarlo y administrarlo de forma adecuada suele ser complicado. Hoy se necesitan nuevos métodos para automatizar de forma más eficaz la mitigación de unas amenazas que no dejan de evolucionar

¿Por qué los WAF tradicionales no son adecuados?

Los firewall de aplicaciones web (WAF) clásicos fueron creados inicialmente para abordar el problema de los servidores de aplicaciones web que utilizaban código vulnerable a multitud de ataques conocidos, como las inyecciones de código XSS (cross-site scripting) y SQL. Los WAF se han estado implementando durante años para abordar estas vulnerabilidades comunes, aunque a menudo con problemas de falsos positivos o complejidad operativa. El WAF original de código abierto, ModSecurity, es a menudo blanco de ataques de bypass o técnicas de evasión que intentan frustrar los mecanismos, en gran parte pasivos y basados en filtros, utilizados para detectar solicitudes maliciosas.

Los firewalls de nueva generación (NGFW) afirman contar con funciones dedicadas a las aplicaciones y ser capaces de detener algunos ataques de inyección (XSS, SQLi, etc.). Sin embargo, estos cortafuegos avanzados siguen basando su detención en filtros pasivos y no examinan cada solicitud HTTP. En realidad, funcionan más bien como un sistema de prevención de intrusiones (IPS), muestreando las solicitudes y examinando sus primeros bytes, en lugar de toda la carga útil de la solicitud. Como resultado, los ataques de bypass en la capa de la aplicación contra las tecnologías NGFW son bastante comunes. Además, las fuentes de reputación de direcciones IP implementadas en los NGFW y otras tecnologías de firewall han demostrado resultar ineficaces contra botnets y otras amenazas automatizadas.

La tecnología WAF ha mejorado mucho con los años, pero se sigue basando ampliamente en técnicas de filtrado pasivo utilizadas para detectar cargas útiles maliciosas y verificar el cumplimiento de protocolos en las solicitudes web. Además, por la complejidad operativa en el manejo de las políticas WAF, muchas empresas han dejado sin protección algunas aplicaciones. Muchos de los ataques más sonados pudieron explotar una vulnerabilidad conocida de una aplicación porque la empresa no logró retocar el servidor de aplicaciones o implementar una política WAF con la suficiente rapidez.

Y por si estos retos no fueran suficiente, la evolución de las tecnologías de automatización y el fácil acceso a redes perversas de bots a sueldo hacen que detectar amenazas sea cada día más difícil. Las tecnologías de automatización como los navegadores sin cabeza hacen que sea difícil distinguir entre usuarios humanos y robots, incluso utilizando CAPTCHAS. Los botnets aprovechan las numerosas debilidades de los dispositivos IoT, módems de cable y navegadores, todos ellos fáciles de infectar. Ante ello, las direcciones IP de origen son poco útiles para detectar y mitigar los ataques de botnets.

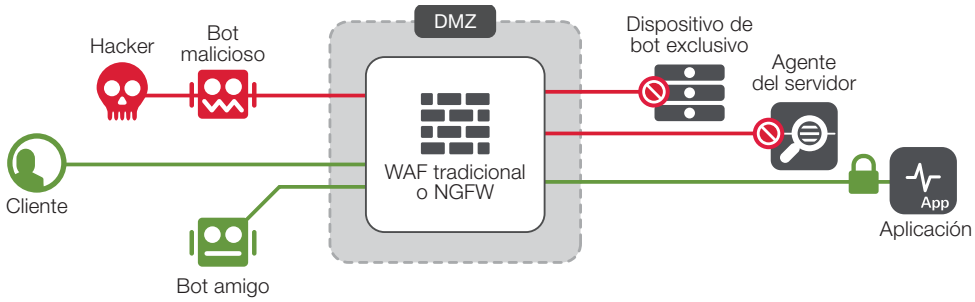

Figura 1: Las amenazas automatizadas son capaces de eludir los WAF tradicionales y los de nueva generación (NGFW.)

Las amenazas automatizadas lideran los ataques actuales.

La fuente de la mayoría de los ataques, sea del tipo que sea, está automatizada. Los ataques DDoS, las violaciones de datos, la detección de vulnerabilidades, el credential stuffing, los ataques de fuerza bruta, la acumulación de recursos, etc., están casi todos automatizados. Los hackers utilizan la automatización para lanzar ataques a gran escala y detectar vulnerabilidades, y ello pese a contar con menos recursos económicos y humanos que las empresas contra quienes actúan. En muchos casos, estos ataques automatizados no contienen una carga útil maliciosa y simplemente buscan eludir las defensas imitando un tráfico legítimo de usuarios.

Los ataques DDoS contra la capa de la aplicación (o capa 7) se han convertido en el vector más frecuente de ataque ya que pueden atacar una URL con muchos recursos con solicitudes legítimas que simplemente sobrecargan la infraestructura de la aplicación. De forma similar, el credencial stuffing (uso automatizado de nombres de usuario y contraseñas robados) y los ataques de fuerza bruta (diseñados para eludir la autenticación de inicio de sesión) son creados por el hacker para simular solicitudes legítimas. Estos ataques de inicio de sesión son a menudo del tipo “low and slow” para evitar ser detectados como un ataque DoS.

El tráfico automatizado malicioso y los bots conforman entre un 30 % y un 40 % del tráfico de un sitio normal, pero también suponen un 90 % o más del tráfico hacia un activo alojado en ese mismo sitio. El objetivo puede ser una página de inicio de sesión (como en los ataques de fuerza bruta o de credential stuffing), o una URL pesada (como en un ataque DDoS contra la capa 7). En un ataque de acumulación de recursos, el hacker suele atacar las páginas donde se compran productos como entradas para eventos, zapatillas u otros. De forma similar, los "scraping" o ataques de extracción de contenido recopilan datos para su posterior explotación. Estos ataques selectivos, además de ser difíciles de detectar, consumen una cantidad desproporcionada de recursos de infraestructura.

Entre las herramientas utilizadas para automatizar estos ataques encontramos navegadores sin cabeza (por ejemplo, Phantom.js y Selenium), escáneres de vulnerabilidades (los mismos que usan los probadores de intrusiones), scripts de línea de comandos, extensiones de navegadores e incluso equipos infectados por malware.

¿El eslabón más débil? El navegador.

Los navegadores suelen ser el eslabón más débil en la seguridad de las aplicaciones. Los hackers intentan infectar a su víctima con ataques de phishing comunes incrustados en mensajes de correo electrónico o en contenidos publicados en redes sociales. Al hacer clic en enlaces maliciosos, el usuario permite al hacker insertar el malware en el equipo de destino. Ese malware puede utilizarse para alistar al equipo infectado en un ejército de botnets y lanzar uno de los ataques mencionados anteriormente.

Con mayor frecuencia, el malware toma la forma de un troyano de acceso remoto (RAT), un registrador de pulsaciones de teclas o algún otro método de recopilación de datos. Estos métodos permiten al hacker hacerse con datos sensibles como credenciales de usuario y contraseñas, listas de contactos y otros datos valiosos en el mercado negro. Proteger al usuario contra el robo de credenciales es una tarea de gran dificultad, especialmente cuando el cliente es un navegador o una aplicación móvil. Este tipo de clientes ofrecen opciones limitadas para aplicar una estrategia de seguridad en sus dispositivos endpoint.

Los usuarios a menudo no saben que su dispositivo ha sido comprometido y siguen pensando que el servicio de Internet está protegiendo sus datos sensibles. Mientras el cifrado HTTPS permite proteger los datos en tránsito, no protege los datos introducidos en el endpoint o punto de acceso del servicio.

Implementar mejores controles de seguridad de aplicaciones.

El WAF tiene que evolucionar hacia un control de seguridad activo, capaz de interrogar al punto de acceso del servicio del cliente y reforzar de forma dinámica la estrategia de seguridad de la aplicación. La buena noticia es que el WAF Avanzado de F5 emplea contramedidas para detectar y detener las amenazas, siempre cambiantes, a la capa de la aplicación. A un nivel superior, el WAF Avanzado de F5 integra el análisis de comportamientos y las inyecciones de código dinámico como sus dos principales mecanismos disponibles para evaluar de forma más completa la amenaza asociada con cualquier sesión del cliente.

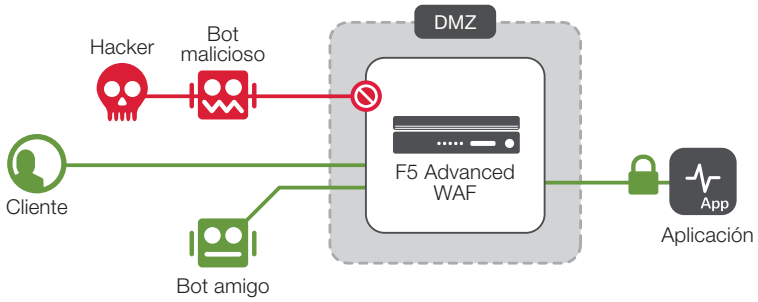

Figura 2: El WAF Avanzado de F5 detecta los bots sin agentes de servidor o dispositivos específicos.

Una vez creados perfiles que establezcan la base de comportamiento normal del tráfico de las aplicaciones, será más fácil detectar los patrones de tráfico anómalos. Al igual que la automatización ha incrementado las capacidades del hacker, estas tecnologías pueden distinguir el tráfico normal del tráfico anómalo mejor de lo que haría un ingeniero de seguridad. El WAF avanzado de F5 utiliza un sistema de análisis avanzado y de aprendizaje automático para generar firmas dinámicas que bloquearán el tráfico malicioso, sin intervención de administrador alguno.

Usando inyecciones JavaScript para saber si un cliente es un navegador usado por un humano, el WAF Avanzado de F5 crea una huella digital del cliente y detecta fácilmente bots y otras herramientas automatizadas. Con las huellas del cliente, se puede seguir al hacker más allá de la dirección IP. La defensa proactiva contra bots del WAF Avanzado de F5 analiza cada sesión del cliente, identificando el tipo cliente así como distinguiendo los bots amigos de los maliciosos. Estos procedimientos no son visibles para el usuario, haciendo que se reduzca o elimine su impacto en la experiencia de usuario (UX) asociada a los CAPTCHAs.

También se puede inyectar código para cifrar dinámicamente las pulsaciones de teclado del usuario, protegiéndole desde su propio dispositivo infectado de malware. La tecnología DataSafe[1] de F5 implementa esta protección para los campos de nombre de usuario y contraseña, evitando así el robo de credenciales. Esta protección es vital ya que el 86 % de las violaciones de datos se dirigen contra la identidad o la aplicación, según una investigación de F5 Labs[2].

Como las API son difíciles de proteger contra ataques automatizados, las API móviles se han convertido cada vez más en un objetivo de los hackers. Con solo la funcionalidad de la aplicación móvil en lugar de un navegador, los desarrolladores de aplicaciones móviles se ven obligados a implementar controles de seguridad más robustos. El nuevo F5 Anti-Bot Mobile SDK[3] permite a las empresas integrar rápidamente las capacidades avanzadas de seguridad en sus aplicaciones móviles actuales en apenas unos clics.

Centrarse en las amenazas automatizadas tiene sus ventajas.

Al poner el foco en las amenazas automatizadas y emplear medidas de seguridad más activas, las empresas pueden lograr beneficios significativos en comparación con los enfoques tradicionales de WAF, entre ellos:

Mejoras operativas

Todas las aplicaciones web comparten navegadores y aplicaciones móviles como clientes, por lo que resulta más fácil implementar una política WAF general para la mayoría de aplicaciones web (idealmente todas). Tener aplicaciones web sin una política WAF o revisiones activas es cosa del pasado.

Reducción de riesgos

Eliminando del arsenal del hacker la posibilidad de hacer escaneos automatizados, le costará más encontrar la última vulnerabilidad en la infraestructura de la aplicación. El riesgo de que un servidor no actualizado quede expuesto desde el primer minuto se reduce drásticamente.

Mejor uso de los recursos

Con una reducción del tráfico de hasta un 40 %, también se reducirá el coste operativo de los servidores de aplicaciones, especialmente en entornos de nube pública. Y con una carga menor, el rendimiento del servidor de aplicaciones y experiencia de usuario también mejorarán. Reducir la carga de base hará que las aplicaciones web sean menos vulnerables a un ataque DDoS en la capa aplicativa.

Los métodos aquí descritos permiten afrontar la seguridad de aplicaciones web de un modo nuevo. Reflejan cómo F5 se enfrenta al cambiante panorama de amenazas. Utilizando un enfoque de seguridad más activo mediante el uso de herramientas como nuestro WAF Avanzado, los profesionales de la seguridad pueden implementar controles más eficaces y proteger más aplicaciones. F5 es pionera en el sector de los cortafuegos avanzados. Esto incluye medidas integrales que mitigan la acción de los bots en sitios web y aplicaciones móviles, protección de credenciales en el navegador y análisis automatizado de comportamientos mediante aprendizaje automático.

[1] https://www.f5.com/pdf/products/application-level_field_encryption_for_credential_and_data_protection.pdf

[2] https://f5.com/labs/articles/threat-intelligence/cyber-security/lessons-learned-from-a-decade-of-data-breaches

[3] https://www.f5.com/pdf/products/integrate_F5_anti-bot_mobile_SDK_with_any_mobile_app.pdf

DC0418 | WP-SEC-222132511