FireEye

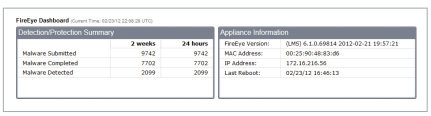
Ficha técnica

Malware Analysis System

Análisis forense de ataques selectivos avanzados de próxima generación

Aspectos destacados

- Racionaliza y agrupa el análisis de los archivos maliciosos, el código web y los ejecutables
- Informes detallados sobre los cambios en sistemas operativos y aplicaciones realizados en sistemas de archivos, memoria y registros
- Análisis en modo de entorno aislado (sandbox) o en tiempo real para confirmar los exploits desconocidos
- Elimina problemas de despliegue y configuración gracias a un entorno preconfigurado, además del montaje y desmontaje automatizados de imágenes de prueba virtuales
- Generación dinámica de información sobre malware para ofrecer protección inmediata a nivel local a través de la integración con Central Management System (CMS)
- Captura de paquetes para permitir el análisis de sesiones con URL maliciosas y la ejecución de código malicioso
- Admite reglas YARA personalizadas (compatible con la versión 1.3)
- Incluye comprobaciones con la suite antivirus para simplificar la priorización de las respuestas ante incidentes
- Admite el acceso a servicios de red AAA de terceros, además de la autenticación local



El panel de MAS muestra el estado (completo y pendiente) del análisis del motor VX

La solución FireEye Malware Analysis System (MAS) proporciona a los analistas de amenazas control práctico sobre potentes entornos de pruebas configurados automáticamente para ejecutar e inspeccionar con seguridad malware avanzado, ataques desconocidos (zero-day) y ataques mediante amenazas persistentes avanzadas (APT) selectivas, que llegan a través de archivos, adjuntos de correo electrónico y objetos web.

Los ciberdelincuentes diseñan sus ataques para penetrar en empresas, cuentas de usuario o sistemas específicos, por lo que los analistas necesitan herramientas de análisis forense sencillas que les ayuden a reaccionar rápidamente frente a actividades maliciosas muy selectivas.

Evaluación de ataques a sistemas operativos, navegadores y aplicaciones

El motor FireEye Virtual Execution (VX) ofrece a los analistas internos una visión completa del ataque, desde el exploit inicial hasta los destinos de devolución de llamadas y los intentos de descarga de archivos binarios posteriores. A través de un entorno de análisis virtual basado en Windows instrumentado y preconfigurado, el motor VX ejecuta completamente el código malicioso para permitir una inspección en profundidad de los formatos de archivo, adjuntos de correo electrónico y objetos web más habituales. FireEye MAS inspecciona archivos individuales o lotes de archivos en busca de malware y supervisa los intentos de conexión salientes en varios protocolos.

Dedicación exclusiva al análisis, no a la administración

El motor VX incluye hardware para PC virtualizado que ejecuta versiones completas de sistemas operativos Windows, así como navegadores, complementos y otras aplicaciones de terceros. El dispositivo MAS ahorra a los administradores una gran cantidad de tiempo, que de otra forma dedicarían a la configuración, análisis del tráfico de red y restauración de los entornos de máquinas virtuales que se utilizan en el análisis de malware manual.

"Uno de los grandes atractivos de la solución de FireEye es que el análisis se realiza en un entorno de ejecución virtual para determinar si una muestra de código seleccionada es de verdad una amenaza. La información detallada que se genera nos permite determinar la opción ideal para resolver un problema. En definitiva, nos permite saber exactamente cómo reaccionar".

— Director de ciberseguridad de una empresa del sector energético

FireEye

Ficha técnica

Modos de análisis en modo de entorno aislado (sandbox) o en modo honeypot

En modo de entorno aislado, los investigadores pueden ver la ruta de ejecución de muestras de malware específicas, así como generar un perfil dinámico y anónimo del ataque, que puede distribuirse a través de CMS a otros dispositivos FireEye Web, Email y File Malware Protection System (MPS). Los perfiles de ataque de malware incluyen identificadores de código de malware, URL de exploits y otras fuentes de infecciones y ataques. Además, las características del protocolo de comunicación del malware se comparten para bloquear de forma dinámica los intentos de filtración de datos.

Además del análisis en un entorno aislado, FireEye ofrece un modo "honeypot" en red y en tiempo real para el análisis del ciclo de vida completo del malware. El malware avanzado actual consigue eludir la seguridad tradicional desencadenando sus ataques en varias etapas. La primera etapa del aprovechamiento de una vulnerabilidad sencillamente establece una "cabeza de puente" para los ciberdelincuentes.

FireEye integra inspecciones del tráfico entrante y saliente en varios protocolos para llevar a cabo un análisis completo y multivectorial de las amenazas a sistemas operativos, la Web, el correo electrónico y las aplicaciones.

Personalización mediante reglas basadas en YARA

La solución MAS admite la importación de reglas YARA personalizadas para especificar reglas a nivel de byte particulares y analizar rápidamente objetos sospechosos en busca de amenazas específicas para la empresa. Las reglas personalizadas se agregan al análisis del motor VX para identificar probables objetos maliciosos, así como objetos ya clasificados como maliciosos.

Red de protección contra el malware global

Los sistemas Malware Analysis Systems pueden compartir automáticamente los datos forenses sobre el malware con otros dispositivos MPS a través de FireEye CMS, con el fin de bloquear los intentos de filtración de datos salientes y neutralizar los ataques entrantes conocidos. Los datos de amenazas de MAS también se pueden compartir a través de FireEye Malware Protection Cloud (MPC) para proteger contra los ataques emergentes.

Gracias a los motores de ejecución virtual preconfigurados, que eliminan la necesidad de ajustar los análisis heurísticos, la solución FireEye MAS ahorra a los administradores tiempo y problemas de configuración. Se trata de una solución asequible y fácil de administrar que ayuda a los investigadores sobre amenazas a analizar los ataques selectivos avanzados sin añadir tiempo de administración de red y de seguridad.

Especificaciones técnicas

	MAS 4310	MAS 7300	MAS 8300
Formato	Montaje en bastidor (1 unidad)	Montaje en bastidor (1 unidad)	Montaje en bastidor (2 unidades)
Peso	13,6 kg	13,6 kg	22,7 kg
Dimensiones (ancho x fondo x alto)	43,7 cm x 65 cm x 4,3 cm	43,7 cm x 65 cm x 4,3 cm	43,7 cm x 70,9 cm x 8,9 cm
Alojamiento	Cabe en bastidor de 19 pulgadas	Cabe en bastidor de 19 pulgadas	Cabe en bastidor de 19 pulgadas
Puertos de administración	(2) Puertos BASE-T 10/100/1000	(2) Puertos BASE-T 10/100/1000	(2) Puertos BASE-T 10/100/1000
Puertos de supervisión	N/D	N/D	(2) Puertos BASE-T 10/100/1000
Rendimiento	Hasta 25.000 objetos al día	Hasta 50.000 objetos al día	Hasta 100.000 objetos al día
Voltaje de entrada (CA)	Conmutación automática, 100 - 240 V de CA, de onda completa	Conmutación automática, 100 - 240 V de CA, de onda completa	Conmutación automática, 100 - 240 V de CA, de onda completa
Corriente de entrada (CA)	8,5 - 6,0 A	8,5 - 6,0 A	9,5 - 7,2 A
Fuente de alimentación/ RAID	Dual 700 W/2 discos (HDD) SAS en hardware RAID1	Dual 700 W/2 discos (HDD) SAS en hardware RAID1	Dual 1400 W/2 discos (HDD) SAS en hardware RAID1
Frecuencia	50 - 60 Hz	50 - 60 Hz	50 - 60 Hz
Temp. de funcionamiento	10 °C a 35 °C	10 °C a 35 °C	10 °C a 35 °C

Nota: todos los valores de rendimiento varían en función de la configuración del sistema y del perfil del tráfico procesado.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408.321.6300 | LATAM@FireEye.com | www.FireEye.com