FIREEYE™

FICHA TÉCNICA

Análisis de Malware

Análisis de ataques con visibilidad total

ASPECTOS DESTACADOS

- Lleva a cabo un análisis forense en profundidad de todo el ciclo de vida del ataque con la ayuda del motor FireEye MVX.
- Racionaliza y organiza en lotes el análisis del código web, los archivos y los ejecutables sospechosos.
- Genera informes detallados sobre los cambios en sistemas de archivos, en la memoria y en los registros a nivel de sistema operativo y de aplicaciones.
- Ofrece un análisis real o en modo sandbox para confirmar los exploits de día cero
- Genera información sobre amenazas de forma dinámica para garantizar de manera inmediata la protección del entorno local a través de la integración con FireEye Central Management
- Captura los paquetes para analizar la ejecución de código y las sesiones a URL maliciosas.
- Incluye FireEye AV-Suite para optimizar el establecimiento de prioridades de la respuesta a incidentes.
- Es compatible con entornos Windows y MacOS X.

Figura 1. Dispositivo AX 5550 de análisis de malware de FireEye.

Descripción general

El análisis de malware de FireEye es una solución de análisis forense que proporciona a los analistas de seguridad un control manual sobre entornos de pruebas potentes autoconfiguradas en los que pueden ejecutar y examinar con total seguridad ataques mediante malware avanzado, amenazas de día cero y amenazas persistentes avanzadas (APT) integrados en páginas web, archivos adjuntos de correo electrónico y archivos.

Los ciberdelincuentes personalizan sus ataques para infiltrarse en una empresa, cuenta de usuario o sistema concretos. Para combatirlos, los analistas necesitan herramientas de investigación forense fáciles de usar que les ayuden a responder rápidamente a estas actividades maliciosas selectivas.

Evaluación de los ataques a sistemas operativos, navegadores y aplicaciones

El análisis de malware (Malware Analysis) utiliza el motor FireEye Multi-Vector Virtual Execution™ (MVX) para proporcionar a los analistas internos con una vista completa de 360 grados de un ataque, desde el exploit inicial a los destinos de devolución de llamada y seguir en los intentos de descarga binaria.

El motor MVX ejecuta completamente el código sospechoso en un entorno de análisis virtual Microsoft Windows y Apple Mac OS X instrumentado y preconfigurado, lo que permite una inspección profunda de archivos, archivos adjuntos de correo electrónico y objetos web comunes. El análisis de malware (Malware Analysis) utiliza este motor MVX para inspeccionar archivos individuales o grupos de archivos en busca de malware y supervisa los intentos de conexión salientes en varios protocolos.

Dedique tiempo al análisis y no a la administración

El análisis de malware (Malware Analysis) libera a los administradores de las tareas tediosas asociadas a la instalación, a la configuración de valores de referencia y a la restauración de los entornos de máquinas virtuales que se utilizan en el análisis manual del malware. Ofrece a los analistas encargados de la investigación forense una función de personalización integrada y control granular de las detonaciones de las cargas útiles, de manera que pueden conseguir una comprensión total del ataque según las necesidades de la empresa.

Análisis en entornos reales o aislados

El análisis de malware brinda a los usuarios dos modos de análisis: en entornos reales o aislados. Los analistas de malware utilizan el modo de red activo en tiempo real para analizar el ciclo de vida completo del malware, permitiendo la conectividad externa. Esto permite al análisis de malware (Malware Analysis) realizar un seguimiento de los ataques avanzados en varias etapas de ejecución y distintos proveedores. En modo sandbox, la ruta de ejecución de muestras de malware está perfectamente aislada y visible en el entorno virtual.

En ambos modos los usuarios pueden generar un perfil dinámico y anonimizado del ataque, que se puede compartir con otras soluciones de FireEye a través de FireEye Central Management. Los perfiles de ataque de malware generados por el análisis de malware incluyen los identificadores del código del malware, las URL del exploit y otras fuentes de infecciones y de ataques. Las características del protocolo de comunicaciones del malware también se comparten a fin de bloquear de forma dinámica los intentos de exfiltración de datos en todo el despliegue de FireEye de la organización a través de la nube FireEye Dynamic Threat Intelligence™ (DTI).

Personalización mediante reglas YARA

El análisis de malware permite la importación de reglas YARA personalizadas para establecer reglas a nivel de byte y analizar rápidamente los objetos sospechosos relacionados con amenazas diseñadas específicamente contra la organización.

Red mundial de protección antimalware

El análisis de malware puede compartir automáticamente los datos de investigación forense sobre malware con otras soluciones de FireEye a través de Central Management, así como bloquear los intentos de exfiltración de datos salientes y neutralizar los ataques conocidos entrantes. Los datos de amenazas del análisis de malware se pueden compartir a través de la nube DTI de FireEye para garantizar la protección contra los nuevos ataques emergentes.

Gracias a los motores FireEye MVX preconfigurados, que eliminan la necesidad de ajuste del análisis heurístico, el análisis de malware permite a los administradores dedicar menos tiempo a problemas de instalación y configuración. Esta solución también ayuda a los investigadores sobre amenazas a analizar los ataques selectivos avanzados sin aumentar los gastos de administración de la seguridad y de la red.

Tabla 1. Especificaciones técnicas.

	AX 5550
Rendimiento*	Hasta 8200 análisis al día
Asistencia OS	Microsoft Windows/Apple Mac OSX
Puertos de interfaz de red	2 puertos 10/100/1000BASE-T
Puerto IPMI (panel posterior)	Incluidos
Teclado	Incluidos
Puertos DB15 VGA (panel posterior)	Incluidos
Puertos USB (panel posterior)	4 puertos USB tipo A
Puerto serie (panel posterior)	115 200 bits/s, sin paridad, 8 bits, 1 bit de parada
Capacidad del disco	2 unidades HDD de 4 TB, RAID 1, 3,5 pulgadas, FRU
Empaque	Montaje en bastidor 1RU, para un rack de 19 in
Dimensiones del chasis (Ancho x Profundidad x Alto)	437 mm (17,2 in) x 650 mm (25,6 in) x 43,2 mm (1,7 in)
Alimentación eléctrica (CC)	No disponible
Alimentación eléctrica (CA)	Redundante (1+1) 750 W, 100 a 240 VCA, 8 a 4,5 A, conector IEC60320-C14 de 50 a 60 Hz, FRU
Consumo máximo de energía	225 W
Disipación térmica máxima	768 BTU/h

Tabla 1. Especificaciones técnicas.

	AX 5550
Tiempo medio entre fallos	54 200 h
Peso neto/embalado kg (lb)	12,2 kg (26,8 lb)/17,2 kg (37,8 lb)
Certificaciones de seguridad	IEC 60950, EN 60950, CSA 60950-00, marcado CE
Certificaciones CEM/IEM	FCC (parte 15, clase A), CE (clase A), CNS, AS/NZS, VCCI (clase A)
Cumplimiento de normativas	RoHS, REACH, WEEE
Temperatura de funcionamiento	0 a 40 °C (32 a 104 °F)
Humedad relativa de funcionamiento	10 a 95 % a 40 °C, sin condensación
Altitud de funcionamiento	3000 m/9842 pies

Nota: Los valores de rendimiento se basan en los tiempos de análisis predeterminados observados durante el uso del análisis de malware, pero variarán en función de la configuración del sistema y de los perfiles de tráfico procesados.

Para obtener más información sobre FireEye, visite: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

Acerca de FireEye, Inc.

FireEye es una empresa de seguridad basada en inteligencia. FireEye, que funciona como una extensión escalable y transparente de las operaciones de seguridad del cliente, ofrece una sola plataforma que combina tecnologías innovadoras de seguridad, inteligencia sobre amenazas similar a los de una Nación y los servicios de consultoría de fama mundial de Mandiant®. Gracias a este enfoque, FireEye elimina la complejidad y la carga de la seguridad cibernética para las organizaciones que desean estar preparadas y responder ante los ataques cibernéticos, además de prevenirlos.

FIREEYE™