FIREEYE™

SCHEDA TECNICA

Analisi del malware

Analizza gli attacchi con visibilità a 360°

CARATTERISTICHE PRINCIPALI

- Analisi forense approfondita per l'intero ciclo di vita di un attacco, utilizzando il motore FireEye MVX
- Ottimizza e raggruppa in batch l'analisi di codice web, eseguibili e file sospetti
- Crea report dettagliati sulle modifiche applicative del sistema operativo a livello di sistema relative a file system, memoria e registri
- Offre analisi in modalità live o sandbox per confermare gli exploit zero-day
- Genera dinamicamente informazioni sulle minacce per una protezione locale immediata tramite l'integrazione con FireEye Central Management
- Acquisisce i pacchetti per consentire l'analisi di sessioni URL ed esecuzione di codice pericolosi
- Include la suite FireEye AV per ottimizzare la prioritizzazione delle risposte agli incidenti
- Include il supporto per gli ambienti Windows e MacOS X

Figura 1. Appliance FireEye Malware Analysis AX 5550.

Panoramica
FireEye Malware Analysis è una soluzione di analisi forense che offre agli analisti della sicurezza un controllo pratico su potenti ambienti di test autoconfigurati per eseguire e analizzare in sicurezza malware avanzato, minacce zero-day e attacchi APT (Advanced Persistent Threat) incorporati all'interno di pagine web, allegati di posta elettronica e file.

Siccome i criminali informatici personalizzano gli attacchi affinché possano penetrare un'azienda specifica, un account utente o un sistema, gli analisti hanno bisogno di strumenti forensi di semplice utilizzo che li aiutino a rispondere tempestivamente alle attività dannose mirate.

Valutazione di attacchi contro sistema operativo, browser e applicazioni
Malware Analysis utilizza il motore FireEye Multi-Vector Virtual Execution™ (MVX) per fornire agli analisti interni una visione completa a 360° di un attacco, dall'exploit iniziale alle destinazioni di callback, e seguire i tentativi di download di codice binario.

Attraverso un ambiente di analisi virtuale Microsoft Windows e Apple Mac OS attrezzato e preconfigurato, il motore MVX esegue in modo completo il codice sospetto per consentire un'analisi approfondita degli oggetti Web comuni, degli allegati di posta elettronica e dei file. Malware Analysis utilizza il motore MVX per analizzare file singoli o blocchi di file alla ricerca di malware e tiene traccia dei tentativi di collegamento in uscita su diversi protocolli.

Più tempo per l'analisi, meno per l'amministrazione
Malware Analysis libera gli amministratori dalle attività, dispendiose in termini di tempo, di impostazione, baselining e ripristino degli ambienti di macchine virtuali utilizzate nell'analisi manuale del malware. Grazie alla personalizzazione e ai controlli granulari integrati sulle destinazioni dei payload, Malware Analysis consente agli analisti forensi di ottenere una comprensione dettagliata dell'attacco in grado di soddisfare le esigenze dell'azienda.

Analisi in modalità live o sandbox

Malware Analysis offre agli utenti due modalità di analisi: live e sandbox. Coloro che analizzano il malware utilizzano la modalità live in rete per l'analisi del ciclo di vita completo del malware, autorizzando la connettività esterna. In questo modo Malware Analysis è in grado di tenere traccia di attacchi complessi in più fasi e vettori differenti. Nella modalità sandbox, il percorso di esecuzione di particolari campioni di malware è incluso e visibile nella sua interezza nell'ambiente virtuale.

In entrambe le modalità, gli utenti possono generare un profilo dinamico e anonimo dell'attacco condivisibile tramite FireEye Central Management con altre soluzioni FireEye. I profili di attacco malware generati da Malware Analysis includono elementi che identificano il codice malware, gli URL dell'exploit e altre fonti di infezione e attacco. Inoltre, vengono condivise le caratteristiche del protocollo di comunicazione del malware per bloccare in modo dinamico i tentativi di esfiltrazione dei dati sull'intera distribuzione FireEye in azienda tramite la soluzione FireEye Dynamic Threat Intelligence™ (DTI).

Le regole basate sullo strumento YARA consentono la personalizzazione

Malware Analysis supporta l'importazione di regole YARA personalizzata per specificare regole a livello di byte e analizzare rapidamente gli oggetti sospetti al fine di individuare eventuali minacce specifiche per l'azienda.

Una rete globale di protezione contro il malware

Malware Analysis può condividere automaticamente i dati forensi sul malware con altre soluzioni FireEye tramite Central Management, bloccare i tentativi di esfiltrazione dei dati in uscita e gli attacchi noti in entrata. I dati sulle minacce ottenuti da Malware Analysis possono essere condivisi attraverso il cloud FireEye DTI per garantire la protezione contro nuovi attacchi emergenti.

Malware Analysis consente agli amministratori di risparmiare tempo nelle attività di configurazione e relative problematiche grazie ai motori FireEye MVX preconfigurati che eliminano la necessità di euristiche di ottimizzazione. Inoltre, questa soluzione aiuta i ricercatori ad analizzare gli attacchi mirati avanzati senza aggiungere ulteriori carichi di gestione di reti e sicurezza.

Tabella 1. Caratteristiche tecniche.

	AX 5550
Prestazioni*	Fino a 8.200 analisi al giorno
Sistema operativo supportato	Microsoft Windows/Apple Mac OSX
Porte interfacce di rete	2 Porte 10/100/1000 BASE-T
Porta IPMI (pannello posteriore)	Inclusa
Tastierino	Incluso
Porte VGA DB15 (pannello posteriore)	Incluse
Porte USB (pannello posteriore)	4 porte USB Tipo A
Porta seriale (pannello posteriore)	115.200 bit/s, nessuna parità, 8 bit, 1 bit di stop
Capacità unità	2 HDD 4 TB, RAID 1, 3,5 pollici, FRU
Involucro	1RU, Rack 19 pollici
Dimensioni chassis (LxPxA)	17,2 po (437 mm) x 25,6 po (650 mm) x 1,7 po (43,2 mm)
Alimentatore CC	Non disponibile
Alimentatore CA	Ridondante (1+1) 750 watt, 100-240 VAC, 8–4,5 A, 50-60 Hz, ingresso IEC60320-C14, FRU
Consumo energetico massimo	225 watt
Dissipazione termica massima	768 BTU/h

Tabella 1. Caratteristiche tecniche.

	AX 5550
MTBF	54.200 h
Peso sola appliance/con confezione, lb (kg)	26,8 lb (12,2 kg)/37,8 lb (17,2 kg)
Certificazioni di sicurezza	IEC 60950, EN 60950, CSA 60950-00, Marchio CE
Certificazioni EMC/EMI	FCC (Parte 15 Classe A), CE (Classe A), CNS, AS/NZS, VCCI (Classe A)
Conformità normativa	RoHS, REACH, RAEE
Temperatura operativa	0–40 °C (32–104 °F)
Umidità operativa relativa	10–95% a 40 °C, senza condensa
Altitudine operativa	3000 m

Nota: I dati relativi alle prestazioni si basano sui tempi di analisi predefiniti utilizzando Malware Analysis, ma varieranno in base alla configurazione di sistema e ai profili di traffico da elaborare.

Per ulteriori informazioni su FireEye, visita il sito Web **www.FireEye.com**

FireEye Italia Srl
Piazza IV Novembre, 7
20124 Milano
Italy
+39 0294750535
italy@FireEye.com

Informazioni su FireEye Italia Srl.
FireEye è un'azienda che offre servizi di sicurezza informatica basati sull'intelligence. Operando come estensione intuitiva e scalabile dei processi operativi di sicurezza dei clienti, FireEye offre un'unica piattaforma in grado di coniugare tecnologie di sicurezza innovative, intelligence sulle minacce a livello nazionale e servizi di consulenza Mandiant® di fama mondiale. Grazie a questo approccio, FireEye elimina la complessità e l'onere della sicurezza informatica per le aziende che hanno difficoltà a prepararsi per futuri attacchi, prevenirli e rispondere ad essi.