McAfee Advanced Threat Defense

Rilevare il malware avanzato

McAfee® Advanced Threat Defense permette alle aziende di rilevare il malware evasivo avanzato e di convertire le informazioni sulle minacce in azioni e protezione immediate. A differenza delle sandbox tradizionali, include funzionalità di analisi aggiuntive che ampliano il rilevamento ed espongono le minacce evasive. La stretta integrazione tra le soluzioni di sicurezza - dalla rete ed endpoint alle attività di indagine - permette una condivisione immediata delle informazioni sulle minacce all'interno dell'ambiente, migliorando protezione e analisi. Opzioni flessibili per la distribuzione supportano ogni tipo di rete.

La nostra tecnologia ha trasformato l'attività di rilevamento collegando le funzioni di analisi avanzata del malware con le difese esistenti, dal perimetro della rete all'endpoint, e condividendo le informazioni sulle minacce con l'intero ambiente IT. Grazie alla condivisione delle informazioni sulle minacce all'interno dell'ecosistema, le soluzioni di sicurezza integrate operano di concerto per interrompere immediatamente le comunicazioni di comando e di controllo, mettere in quarantena i sistemi compromessi, bloccare le ulteriori istanze della stessa minaccia o similare, valutare l'impatto e agire.

McAfee Advanced Threat Defense: rilevamento delle minacce avanzate

McAfee Advanced Threat Defense rileva il malware zero-day furtivo odierno con un innovativo approccio a più livelli. Combina motori di analisi low-touch come firme antivirus, reputazione ed emulazione in tempo reale con l'analisi dinamica (sandboxing) per analizzare il comportamento effettivo. L'indagine continua con un'analisi statica dettagliata del codice che esamina gli attributi del file e i gruppi di istruzioni per stabilire il comportamento previsto o evasivo e valuta la somiglianza con le famiglie di malware note. Come passo finale dell'analisi, McAfee Advanced Threat Defense cerca in modo specifico indicatori dannosi che sono stati identificati attraverso l'apprendimento automatico tramite una profonda rete neurale. Insieme, rappresentano la protezione più efficace disponibile sul mercato contro il malware avanzato in grado di bilanciare efficacemente le esigenze in termini di controllo approfondito e prestazioni.

Principali elementi di differenziazione di McAfee Advanced Threat Defense

Ampia integrazione delle soluzioni

- Integrazione con le soluzione McAfee esistenti, gateway email di terze parti e altri prodotti che supportano gli standard aperti
- Colma in tutta l'azienda le lacune esistenti fra scoperta, contenimento e protezione
- Semplifica i flussi di lavoro per velocizzare risposta e remediation
- Abilita l'automazione

Potenti funzioni di analisi

- Combina analisi approfondita del codice statico, analisi dinamica e apprendimento automatico per un rilevamento più accurato che produce dati d'analisi impareggiabili.
- Funzioni avanzate supportano il SOC e abilitano le attività di indagine

Seguici su:

Mentre i metodi a minore intensità analitica, quali le firme e l'emulazione in tempo reale, favoriscono le prestazioni grazie all'individuazione più semplice del malware identificato, aggiungendo alla sandbox l'analisi statica completa del codice e le informazioni dettagliate ottenute tramite l'apprendimento automatico si amplia il rilevamento di minacce evasive, altamente mimetizzate. Gli indicatori dannosi che potrebbero non essere eseguiti in un ambiente dinamico possono essere identificati attraverso la decompressione, l'analisi statica approfondita del codice e le informazioni dettagliate dell'apprendimento automatico.

Gli autori del malware usano la compressione per cambiare la composizione del codice o per occultarlo al fine di eludere il rilevamento. La maggior parte dei prodotti non è in grado di decomprimere correttamente l'intero codice eseguibile originale (il codice sorgente) per analizzarlo. McAfee Advanced Threat Defense include funzionalità esaurienti di unpacking che rimuovono l'offuscamento, rivelando il codice eseguibile originale. Consente l'analisi statica approfondita del codice per cercare eventuali anomalie, esaminando tutti gli attributi e i gruppi di istruzioni fino a prevedere il reale comportamento del codice stesso.

L'analisi statica approfondita del codice, l'apprendimento automatico e l'analisi dinamica, combinate insieme, offrono una valutazione completa e dettagliata del malware sospetto. Risultati d'analisi impareggiabili producono report riepilogativi che permettono un'ampia comprensione e la definizione delle priorità di azione, e report più dettagliati che forniscono dati approfonditi sul malware.

Miglioramento della protezione

La stretta integrazione fra McAfee Advanced Threat Defense e i dispositivi di sicurezza – dal perimetro della rete all'endpoint – consente a questi ultimi di eseguire immediatamente un'azione quando McAfee Advanced Threat Defense classifica un file come dannoso. Questa stretta integrazione automatizzata fra rilevamento e protezione è fondamentale.

McAfee Advanced Threat Defense può integrarsi in modi diversi: direttamente con soluzioni di sicurezza selezionate, attraverso McAfee Threat Intelligence Exchange o il modulo McAfee Advanced Threat Defense Email Connector.

L'integrazione diretta consente alle soluzioni di sicurezza di agire immediatamente sui file individuati da McAfee Advanced Threat Defense. Incorporano istantaneamente le informazioni sulle minacce nei processi esistenti di imposizione delle policy, impedendo l'ingresso nella rete delle istanze aggiuntive degli stessi file o simili.

I file malevoli individuati da McAfee Advanced Threat Defense compaiono nei registri e nelle dashboard dei prodotti integrati, come se l'intera analisi fosse stata eseguita da essi, semplificando i flussi di lavoro e consentendo agli amministratori di gestire in maniera efficiente gli allarmi tramite una singola interfaccia.

L'integrazione con McAfee Threat Intelligence Exchange amplia le capacità di McAfee Advanced Threat Defense aggiungendo ulteriori difese, come McAfee Endpoint Protection. Abilita inoltre una vasta gamma di soluzioni di sicurezza integrate per accedere ai risultati delle

Distribuzione centralizzata flessibile

- Riduzione dei costi con la distribuzione centralizzata che supporta molteplici protocolli.
- Opzioni flessibili per la distribuzione supportano ogni tipo di rete

Soluzioni integrate

- McAfee® Active Response
- McAfee® Advanced Threat Defense Email Connector
- McAfee® Enterprise Security Manager
- McAfee® ePolicy Orchestrator®
- McAfee® Network Security Platform
- McAfee® Threat Intelligence Exchange
  - McAfee® Application Control
  - McAfee® Endpoint Protection
  - McAfee® Security for Email Servers
  - McAfee® Server Security
- McAfee® Web Gateway
- Bro Network Security Monitor
- TAXII (Trusted Automated eXchange of Indicator Information)

analisi e agli indicatori di compromissione. Se un file viene giudicato dannoso da McAfee Advanced Threat Defense, McAfee Threat Intelligence Exchange ne pubblica immediatamente le informazioni, inviando un aggiornamento della reputazione a tutte le contromisure integrate nell'organizzazione.

Gli endpoint abilitati da McAfee Threat Intelligence Exchange riescono a bloccare le primissime installazioni del malware, permettendo quindi una protezione tempestiva nel caso in cui il file ricompaia in seguito. I gateway abilitati da McAfee Threat Intelligence Exchange impediscono al file di penetrare nell'azienda. Anche se scollegati dalla rete, gli endpoint abilitati da McAfee Threat Intelligence Exchange continuano a ricevere gli aggiornamenti sui file riconosciuti come malevoli, eliminando i punti ciechi dalla consegna fuori banda dei payload.

Il modulo McAfee Advanced Threat Defense Email Connector permette a McAfee Advanced Threat Defense di ricevere gli allegati email ai fini dell'analisi da un gateway di posta. McAfee Advanced Threat Defense analizza i file negli allegati e restituisce una risposta a tutti i gateway di posta attivi all'interno dell'intestazione del messaggio. Il gateway di posta può quindi agire in base alle policy, cancellando o mettendo in quarantena l'allegato, evitando così che il malware infetti e si diffonda sulla rete interna. Una modalità offline consente di consegnare all'utente finale email con allegati durante la scansione con McAfee Advanced Threat Defense. Il gateway email non attende una risposta relativamente all'allegato. Gli amministratori visualizzano i risultati della scansione degli allegati attraverso McAfee Advanced Threat Defense o McAfee Threat Intelligence Exchange. Per il rilevamento avanzato sul server di posta elettronica, McAfee Advanced Threat Defense si integra con McAfee Security for Email Servers tramite McAfee Threat Intelligence Exchange.

Condivisione delle minacce per migliorare e automatizzare il processo di analisi

Per analizzare e porre rimedio ad un attacco, le aziende hanno bisogno di visibilità completa, con informazioni fruibili, al fine di prendere decisioni migliori e reagire nel modo appropriato. McAfee Advanced Threat Defense produce un'intelligence delle minacce approfondita che viene facilmente condivisa nell'intero ambiente per migliorare e automatizzare le attività di analisi. Il supporto per Data Exchange Layer (DXL) e le API REST facilita le integrazioni con altri prodotti e standard di condivisione delle minacce diffusi, come Structured Threat Information eXpression (STIX)/ Trusted Automated eXchange of Indicator Information (TAXII), e permette alle aziende di creare, supportare ed ampliare un ecosistema di sicurezza collaborativo.

All'interno di un ecosistema McAfee, McAfee Enterprise Security Manager utilizza e correla la dettagliata reputazione dei file con gli eventi di esecuzione provenienti da McAfee Advanced Threat Defense e da altri sistemi di sicurezza. Si ottengono così delle visualizzazioni avanzate degli allarmi e della cronologia che potenziano le informazioni di sicurezza, l'ordinamento dei rischi per priorità e la consapevolezza della situazione in tempo reale. Con dati relativi agli indicatori di compromissione provenienti da McAfee Advanced Threat Defense, McAfee Enterprise Security Manager tornerà indietro fino a sei mesi alla ricerca di indicazioni di tali reperti in qualsiasi dato di rete o sistema abbia conservato.

Può svelare sistemi che hanno precedentemente comunicato con fonti di malware identificate di recente. La stretta integrazione con McAfee Endpoint Protection, McAfee Threat Intelligence Exchange e McAfee Active Response ottimizza la risposta e l'efficienza delle operazioni di sicurezza con visibilità e interventi di mitigazione proattiva dei rischi come la creazione di nuove configurazioni, l'implementazione di nuove policy, la rimozione di file e la distribuzione degli aggiornamenti software. Interviene sulla base delle informazioni disponibili quando gli endpoint infetti sulla rete vengono identificati da McAfee Active Response ed elencati nei report di McAfee Advanced Threat Defense. L'efficienza dell'analista aumenta quando questi report dettagliati vengono visualizzati da un singolo spazio di lavoro all'interno di McAfee Active Response.

Funzionalità avanzate a supporto delle analisi

McAfee Advanced Threat Defense offre numerose funzionalità avanzate, tra cui:

- **Supporto configurabile per il sistema operativo e le applicazioni:** personalizza le immagini di analisi con variabili ambientali selezionate per convalidare le minacce e sostenere l'attività di indagine.
- **Modalità utente interattiva:** permette agli analisti di interagire direttamente con gli esempi di malware.
- **Funzioni estese di decompressione:** riducono il tempo di analisi da giorni a minuti.
- **Percorso logico completo:** permette un'analisi più approfondita degli esempi forzando l'esecuzione di percorsi logici aggiuntivi che rimangono dormienti all'interno di tipici ambienti sandbox.
- **Consegna dell'esempio a molteplici ambienti virtuali:** velocizza l'analisi stabilendo quali variabili ambientali sono necessarie per l'esecuzione del file.
- **Reportistica dettagliata:** fornisce informazioni critiche per le indagini tra cui mappatura MITRE ATT&CK™, output di disassemblaggio, immagini della memoria, diagrammi di chiamata con funzioni grafiche, informazioni sui file incorporati o distribuiti, log delle API utente e informazioni PCAP. Le linee temporali delle minacce consentono di visualizzare le fasi di esecuzione degli attacchi.
- **Integrazione con Bro Network Security Monitor:** distribuisce il sensore Bro a un segmento di rete sospetto per monitorare e acquisire il traffico e inoltrare i file a McAfee Advanced Threat Defense per il controllo.

Distribuzione

Opzioni flessibili per l'analisi avanzata delle minacce supportano ogni tipo di rete. McAfee Advanced Threat Defense è disponiile come appliance in locale o virtuale, con supporto per cloud sia privati che pubblici con disponibilità nell'Azure Marketplace.

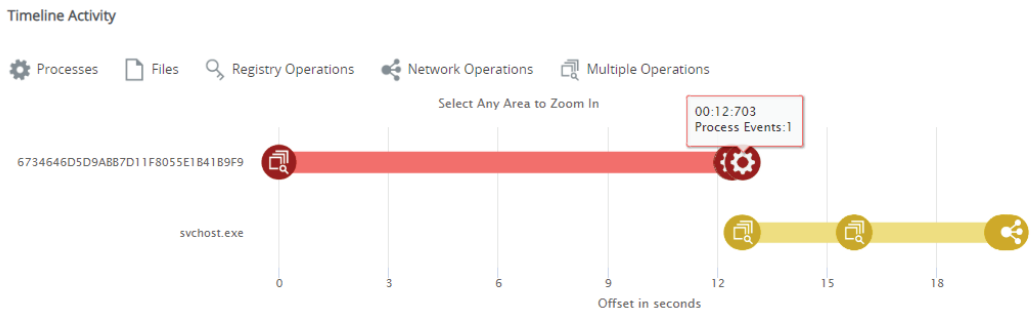

Figura 1. L'attività della timeline visualizza l'esecuzione dei passaggi della minaccia analizzata.

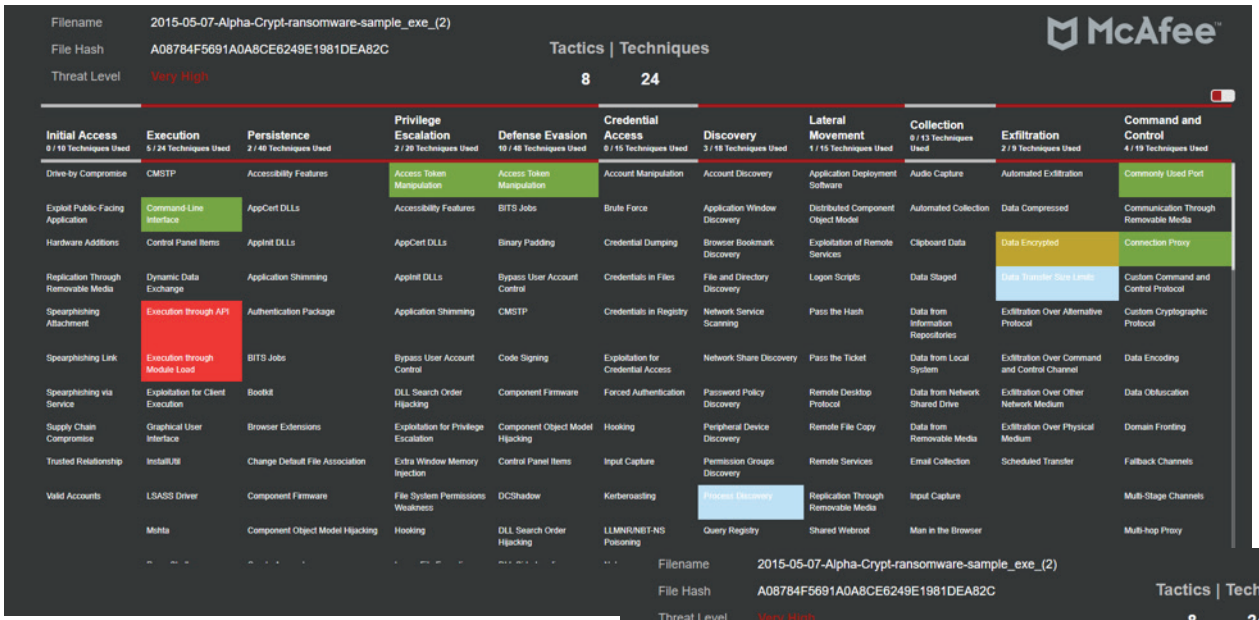

Figura 2. I risultati corrispondono al framework MITRE ATT&CK™.

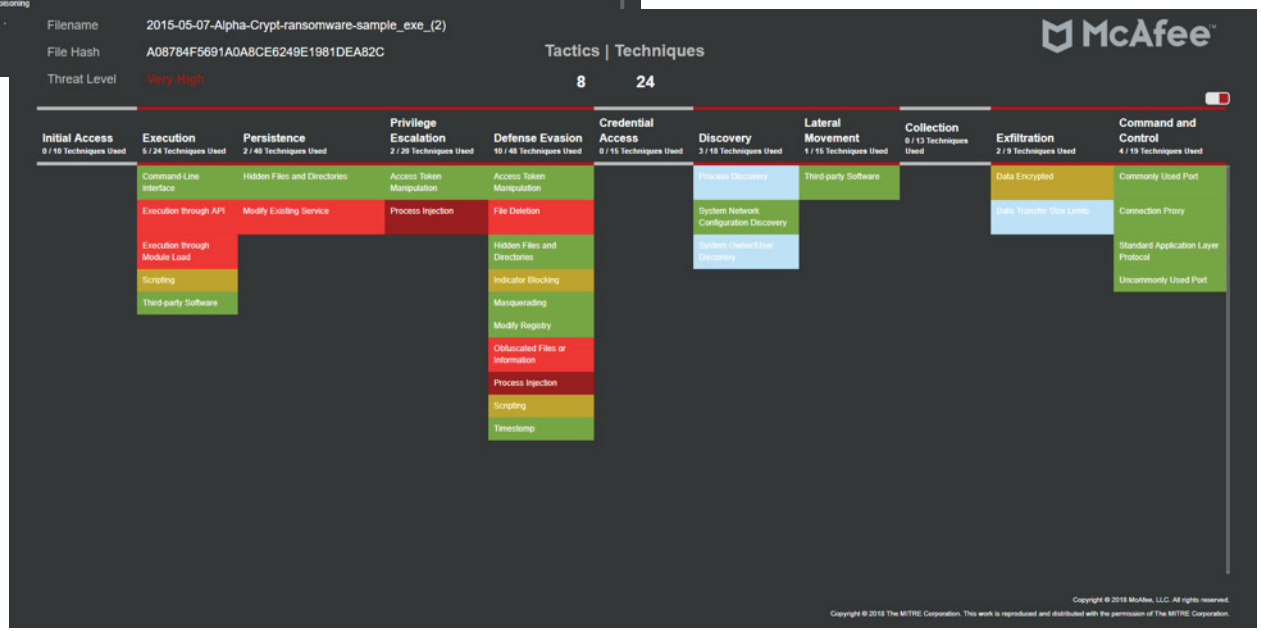

Figura 3. Una vista filtrata dei risultati visualizzati nella figura 2 concentra il report sulle tecniche identificate.

Specifiche tecniche di McAfee Advanced Threat Defense		
Fattore forma fisico	ATD-3200 1U montabile a rack	ATD-6200 1U montabile a rack
Fattore forma virtuale	v1008 ESXi 5.5, 6.0, 6.5, 6.7 Hyper-V Windows Server 2012 R2, Windows Server 2016	
Rilevamento		
Tipi di esempi di file supportati	File PE, file Adobe, file Microsoft Office Suite, file immagine, file compressi, Java, Android Application Package, URL	
Metodi di analisi	McAfee Anti-Malware Engine, reputazione GTI: file/URL/IP, Gateway Anti-Malware (emulazione e analisi comportamentale), analisi dinamica (sandboxing), analisi approfondita del codice, regole YARA personalizzate, apprendimento automatico	
Sistemi operativi supportati	Windows 10 (64 bit), Windows 8.1 (64 bit), Windows 8 (32 bit/64 bit), Windows 7 (32 bit/64 bit), Windows XP (32 bit/64 bit), Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, Windows Server 2003, Android Il supporto per tutti i sistemi operativi Windows è disponibile in tutte le lingue.	
Formati output	STIX, OpenIOC, XML, JSON, HTML, PDF, testo	
Metodi di presentazione	Integrazioni di prodotti specifici non integrati, API RESTful, invio manuale e modulo McAfee Advanced Threat Defense Email Connector (SMTP)	

Ulteriori informazioni

Per ulteriori informazioni o per iniziare un periodo di valutazione di McAfee Advanced Threat Defense, contatta il tuo rappresentante o visita il sito **www.mcafee.com/enterprise/it-it/products/advanced-threat-defense.html**.

Via Fantoli, 7
20138 Milano
Italy
(+39) 02 554171
www.mcafee.com/it