MANDIANT®

PANORAMICA DELLA SOLUZIONE

Contenimento delle minacce strategiche da Ransomware con Mandiant Managed Defense

VANTAGGI

- **Visualizzazione degli avvisi rilevanti**
  Affidati a un esperto per monitorare le segnalazioni di carattere tecnologico in tutto il tuo ambiente e per identificare, analizzare e stabilire le priorità. Otterrai una serie di priorità, arricchite da un contesto.
- **Rileva gli aggressori nascosti**
  Individua le violazioni nascoste e i potenziali attacchi informatici con una ricerca proattiva delle minacce mappata nel quadro del MITRE ATT&CK.
- **Interruzione e risposta rapida**
  Gli esperti di Managed Defense supportano la tua risposta agli attacchi con la conoscenza e l'esperienza del personale specializzato nell'Incident Response di Mandiant e degli analisti della sicurezza.
- **Miglioramento delle prestazioni del tuo team**
  Il nostro team di esperti in sicurezza offre formazione, consulenza e collaborazione al tuo team, fornendo conoscenze in materia di sicurezza informatica di alto livello e una esaustiva comprensione dell'ambiente.
- **Potenziamento delle difese**
  Migliora il tuo livello di sicurezza con valutazioni e raccomandazioni costanti, basate su informazioni rilevanti sulle minacce.

Dal 2017 gli attacchi ransomware sono aumentati rapidamente per frequenza e pericolosità. Quello che inizialmente era considerato un inconveniente è stato adottato da sofisticati attaccanti in attacchi complessi e in più fasi che uniscono la crittografia dei dati e la minaccia della loro diffusione. Nello stesso arco di tempo, questi attaccanti hanno esteso il loro raggio d'azione, passando da un'ampia diffusione delle minacce malware ad attacchi mirati a organizzazioni e a settori specifici, comprese intere città. Oggi, il costo totale di un attacco Ransomware può raggiungere milioni di dollari.

Questa minaccia evoluta ha spinto molte organizzazioni a valutare, sviluppare e aggiornare potenziali tattiche anti-Ransomware per accelerare la loro risposta. Un'efficace capacità di rilevamento e risposta gestiti (Managed Detection and Response, MDR), come Mandiant Managed Defense, può mitigare il rischio di minacce di tipo Ransomware distribuite strategicamente dai gruppi APT, e assicurare ai vertici aziendali e ai consigli di amministrazione la presenza di adeguate capacità di sicurezza. Ottenere queste funzionalità in house può richiedere tempo e risorse.

Managed Defense aiuta a combattere il Ransomware

Alle organizzazioni che si trovano ad affrontare tattiche di ransomware e minacce avanzate, Managed Defense offre il supporto di esperti che ogni giorno lottano contro avversari motivati.

Conoscere le minacce rilevanti per tutti i Threat Vectors

Gli aggressori che vogliono utilizzare il Ransomware possono infiltrarsi nell'ambiente di una vittima tramite una serie di vettori di minacce, tra cui il Remote Desktop Protocol, le e-mail di spear-phishing con link o allegati dannosi, o attraverso un download inconsapevole da un sito web dannoso. Dopo aver compromesso l'ambiente, gli attaccanti individuano i sistemi e i dati chiave per massimizzare le possibilità di successo della loro missione.

Per la maggior parte delle organizzazioni, acquisire visibilità e controllo sull'intera azienda, dalla miriade di endpoint fino all'attuale perimetro di rete in rapida estensione, è fondamentale per individuare la presenza di attacchi sofisticati, post compromissione. Piuttosto che fermarsi agli endpoint, Managed Defense mantiene la visibilità della rete end-to-end per individuare i comportamenti anomali e dare priorità agli avvisi estremamente importanti per le indagini. Inoltre, gli esperti di Mandiant possono utilizzare l'attività di posta elettronica per identificare i nuovi trend degli attaccanti e i nuovi meccanismi di consegna del Ransomware.

Riconoscere gli schemi delle minacce Ransomware

Per un'organizzazione è più importante che mai disporre di analisti esperti con conoscenza su tattiche, tecniche e procedure degli attacchi Ransomware. Per raggiungere i loro obiettivi, gli attaccanti devono prima di tutto creare un punto d'appoggio e poi assicurare la connessione con l'ambiente della vittima. Ad esempio, gli esperti di Mandiant hanno scoperto che gli attaccanti MAZE hanno installato dei payload su numerosi server e postazioni dopo essersi spostati lateralmente, attraverso le reti delle vittime. Il gruppo è stato quindi in grado di ottenere e mantenere l'accesso, incrementare i privilegi e iniziare a spostarsi lateralmente.

Nel 2019, Mandiant ha scoperto che per il Ransomware distribuito strategicamente dai gruppi di minacce APT tra i clienti di Incident Response, il tempo medio di permanenza prima della sua implementazione era di 72 giorni. Anche i clienti di Managed Defense sono stati presi di mira con il Ransomware dai gruppi di minacce APT, ma in quasi tutti i casi il componente Ransomware è stato rilevato e attenuato prima di essere implementato. Questo ha ridotto il tempo medio di permanenza nei sistemi dei clienti da 72 giorni a meno di 24 ore (Fig. 1).

Figura 1.

Nel 2019, Managed Defense ha ridotto in modo significativo il tempo di permanenza del Ransomware strategico per i clienti.

Per individuare un tale attacco strategico di tipo ransomware, le organizzazioni devono prima scoprire questi aggressori nascosti; molte organizzazioni non dispongono di esperti capaci di individuare le minacce e con conoscenze specifiche sul comportamento attuale e storico degli attaccanti. Durante la ricerca di minacce strategiche di tipo ransomware, i team di Managed Defense dedicati alla ricerca delle minacce informatiche si affidano a informazioni approfondite, acquisite in prima linea, e a un'esperienza unica nella risposta agli incidenti.

Reagire prima dell'impatto

Poiché il Ransomware strategico può infettare e crittografare molto rapidamente, è fondamentale rispondere in modo veloce ed efficace. La vasta portata dei recenti attacchi Ransomware richiede ai team della sicurezza di determinare l'intera portata dell'attività degli attaccanti e di intervenire in modo efficace. Managed Defense offre il monitoraggio 24 ore su 24 e la prioritizzazione degli allarmi; in questo modo, un allarme prioritario può essere rapidamente analizzato e valutato da un esperto Mandiant.

Managed Defense sfrutta più di 15 anni di esperienza nella risposta agli incidenti di alto profilo per fornire valutazioni rapide e contenere le minacce. I consulenti di Managed Defense lavorano con gli specialisti in Incident Response di Mandiant per scoprire e fermare l'attività degli aggressori nell'ambiente dei clienti. Questo tipo di risposta rapida evita ai clienti di sostenere il costo di una risposta all'incidente completa nel 98% dei casi. I risultati di Managed Defense vengono elaborati insieme alle informazioni fornite dal tuo team e rese disponibili tramite relazioni dettagliate sul portale di Managed Defense.

Per maggiori informazioni su come Mandiant Managed Defense può aiutare la tua organizzazione a scoprire i Ransomware e come reagire, visita **www.fireeye.com/managed-defense**

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

Informazioni sulle Soluzioni Mandiant

Le Soluzioni Mandiant offrono esperienza di prima linea e intelligence sulle minacce leader di mercato, con funzionalità di security validation in grado di fornire alle organizzazioni gli strumenti necessari per aumentare l'efficacia della sicurezza e ridurre i rischi aziendali.

MANDIANT®

MD-EXT-SB-US-EN-000335-01