SCHEDA TECNICA

Red Team Operations (RTO)

Metti alla prova la tua capacità di proteggere le risorse aziendali più preziose da un attacco mirato al mondo reale

VANTAGGI

- Sapere se i tuoi dati importanti sono a rischio e con quale facilità un agente dannoso è in grado di sottrarli
- Valutare la sicurezza del tuo ambiente a fronte di un autore di un attacco realistico "senza restrizioni"
- Mettere alla prova la capacità del tuo team di sicurezza interno per prevenire, individuare e rispondere a incidenti in un ambiente controllato e realistico
- Individuare e mitigare le vulnerabilità complesse della sicurezza prima che un aggressore le sfrutti
- Ottenere analisi e consigli sui rischi basati sui fatti per migliorare il livello di sicurezza

Perché Mandiant

Mandiant, una società FireEye, è in prima linea nello sviluppo di soluzioni per la sicurezza e l'intelligence informatica dal 2004. I nostri esperti di sicurezza hanno dovuto contrastare le violazioni più complesse del mondo. Conosciamo in dettaglio sia le minacce esistenti che quelle emergenti, così come la rapida evoluzione delle tattiche, delle tecniche e delle procedure utilizzate dagli hacker.

Panoramica del servizio

Le operazioni del Red Team consistono in uno scenario di attacco realistico "senza restrizioni" al vostro ambiente. Il nostro red team di Mandiant ricorre a qualsiasi metodo non distruttivo per raggiungere una serie di obiettivi concordati simulando il comportamento dell'aggressore. Il red team imita da vicino i metodi di attacco attivi e furtivi di un vero aggressore usando le TTP su coinvolgimenti di risposta agli incidenti reali e recenti. Questo aiuta a valutare la capacità del team di sicurezza di rilevare e rispondere a uno scenario di un aggressore attivo.

Esempi di obiettivi		
Sottrarre le e-mail di dirigenti o sviluppatori	Entrare in un ambiente segmentato contenente dati importanti o sensibili dell'attività	Prendere il controllo di un dispositivo automatizzato come un dispositivo IoT, un dispositivo medico o un dispositivo di produzione

Metodologia

Le operazioni del red team iniziano stabilendo congiuntamente se il red team deve conoscere o no l'ambiente. Mandiant applica la propria esperienza nel settore per identificare gli obiettivi che rappresentano i rischi maggiori per le tue principali attività aziendali.

Le operazioni del red team consistono nel seguire le fasi del ciclo vitale degli attacchi.

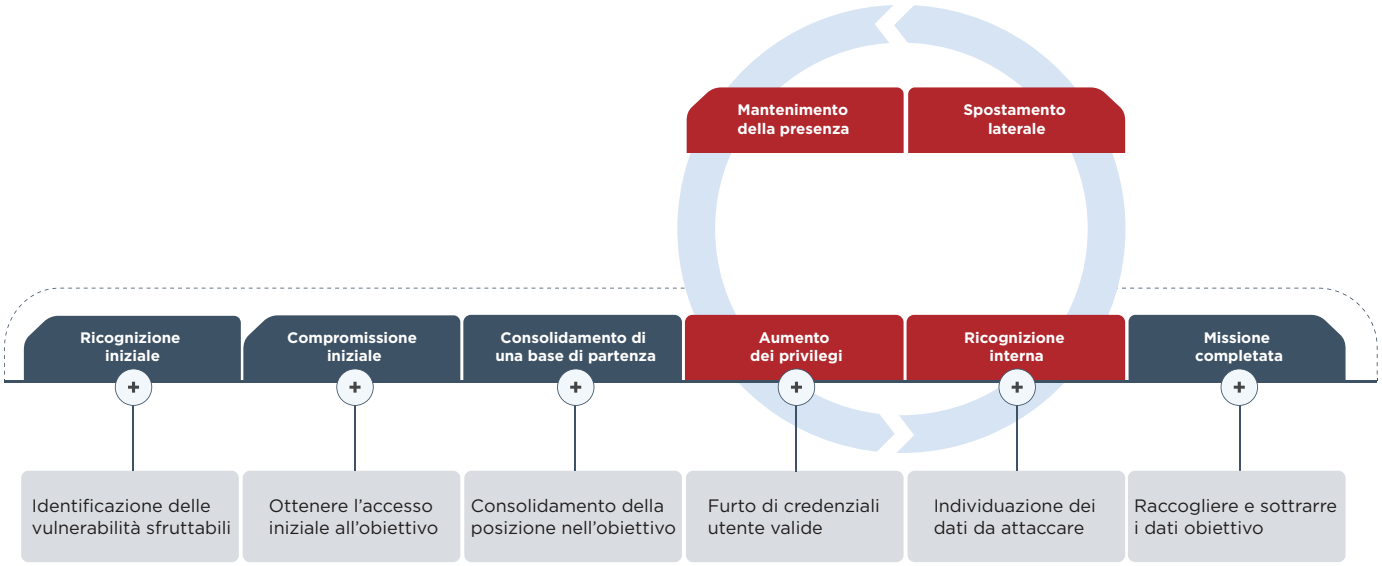

Figura 1. Ciclo di vita di un attacco.

Una volta stabiliti gli obiettivi, il red team inizia effettuando una ricognizione iniziale. Mandiant sfrutta una combinazione di repository di informazioni di proprietà così come strumenti e tecniche di informazioni open source (OSINT) per eseguire la ricognizione dell'ambiente di destinazione.

Mandiant tenta di ottenere l'accesso iniziale all'ambiente di destinazione sfruttando le vulnerabilità o conducendo un attacco di ingegneria sociale. Mandiant sfrutta le tecniche utilizzate dagli aggressori del mondo reale per ottenere un accesso privilegiato a questi sistemi.

Una volta ottenuto l'accesso, il red team tenta di aumentare i privilegi per stabilire e mantenere la persistenza nell'ambiente distribuendo un'infrastruttura di comando e controllo, proprio come farebbe un utente malintenzionato.

Dopo che la persistenza e i sistemi di comando e controllo sono stati stabiliti nell'ambiente, il red team cerca di raggiungere i propri obiettivi con qualsiasi mezzo non distruttivo necessario.

Perché scegliere le operazioni del red team

Le operazioni del red team sono consigliate per organizzazioni che vogliono:

- *Mettere alla prova capacità di rilevamento e di risposta.* I team di sicurezza si preparano per gli incidenti del mondo reale, ma è necessario confermare che possono rispondere correttamente — senza un reale rischio.
- *Aumentare la consapevolezza e mostrare l'impatto.* Il red team Mandiant si comporta come un aggressore del mondo reale, lavorando per compromettere il tuo ambiente tramite Internet e utilizzando le informazioni disponibili solo in rete. Il successo del red team può aiutare a giustificare maggiori budget di sicurezza e identificare lacune che richiedono ulteriori investimenti.

CHE COSA SI RICEVE

- Riepilogo per management e quadri dirigenziali
- Dettagli tecnici con informazioni dettagliate che consentono di ricreare i nostri risultati
- Analisi dei rischi basata sui fatti, in modo da capire se un risultato importante è significativo per il tuo ambiente
- Raccomandazioni di natura tattica per avviare un'ottimizzazione immediata
- Raccomandazioni strategiche per un'ottimizzazione a lungo termine
- Esperienza inestimabile nella capacità di risposta a un incidente realistico senza la pressione di una violazione potenzialmente grave

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

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

Informazioni su FireEye, Inc.
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.