Cyber Deception

CYMMETRIA MAZERUNNER

La strategia dell'inganno per fermare il Cyber Crime

La maggior parte degli attacchi Cyber segue uno schema ricorrente:

- una **fase di ricognizione**, in cui l'attaccante seleziona gli ambienti e le risorse più vulnerabili e nello stesso tempo più "preziose";
- il cosiddetto **movimento laterale**, con cui l'attaccante si sposta da un sistema all'altro fino a raggiungere il suo obiettivo;
- una **fase di raccolta ed estrazione**, con cui l'attaccante si impadronisce delle informazioni.

Cymmetria Mazerunner usa una strategia basata sull'inganno (**deception**) per organizzare la difesa dagli attacchi Cyber. Il fattore chiave di questa strategia si fonda proprio sullo schema ricorrente sopra descritto e consiste nella capacità di **attrarre gli attaccanti all'interno di ambienti controllati** e contestuamente nell'allertare i difensori della minaccia esistente, dando loro il tempo necessario a mettere in campo le adeguate contromisure per neutralizzarla.

Cymmetria MazeRunner è in grado di individuare gli attacchi quando sono ancora nella fase ricognitiva e di condizionare il movimento laterale, **inserendo "esche"** sui percorsi critici, così da attrarre l'attaccante verso un ambiente controllato.

Nello stesso tempo, **Cymmetria MazeRunner**, agisce per facilitare la neutralizzazione della minaccia, comunicando con l'architettura di difesa esistente e fornendo tutte le informazioni necessarie per creare **un'impronta dell'attacco**.

Strategia di Difesa

La strategia di difesa adottata da Cymmetria MazeRunner, può essere riassunta nei seguenti punti.

- **Rilevamento affidabile - attrae gli attaccanti all'interno di ambienti controllati e crea un'impronta dell'attacco.**
- **Efficacia della risposta - fornisce dati e informazioni approfondite, come la fonte dell'attacco e gli strumenti utilizzati dall'attaccante.**
- **Focus sugli alert reali - genera alert reali ed affidabili, evitando i "falsi positivi".**
- **Neutralizzazione - raccoglie informazioni, anche di carattere forense, sugli attacchi e si integra con gli strumenti esistenti per mettere in quarantena l'attacco.**

*La strategia di difesa utilizzata da **Cymmetria MazeRunner** è una strategia basata sull'inganno e sulla promessa di ottenere un vantaggio inaspettato. E' una strategia mutuata dal Cyber Crime che usa l'inganno per mettere a punto le propria azioni criminose: **la preda diventa cacciatore**.*

*Attraverso delle piccole esche, le **Breadcumbs** (briciole di pane) l'attaccante viene indirizzato verso le trappole, i **Decoys Running Service**, dove viene attivato il processo di notifica e la raccolta di informazioni di dettaglio, in grado di creare un'impronta dell'attacco e favorire la sua definitiva neutralizzazione.*

Architettura

L'architettura di Cymmetria MazeRunner, basata su appliance fisiche e virtuali, è uno dei punti di forza dell'applicazione, perché consente una rapida implementazione della soluzione, senza seri impatti di tipo "sistemistico":

- **Un'interfaccia centrale di gestione basata su web.**
- **Breadcumbs - elementi passivi costituiti da dati "attrattivi" per un attaccante (es.Cookie, credenziali RDP e SSH, mapping di cartelle condivise, script OpenVPN…), che vengono distribuiti sulle postazioni di lavoro per essere facilmente trovati dagli attaccanti, durante la fase di ricognizione.**
- **Decoys Running Service - macchine virtuali che hanno la funzione di attrarre l'attaccante in un ambiente controllato; hanno le sembianze e si comportano come ambienti di produzione, e quando un attaccante approda su essi, seguendo le informazioni contenute in un Breadcumbs, viene attivato il processo di notifica e la raccolta di informazioni di dettaglio.**
- **Componenti che consentono l'integrazione con i tool che costituiscono l'ecosistema di Cyber Security, tra cui il SOC o le soluzioni di Threat Intelligence.**

PRINCIPALI BENEFICI

Domina il Nemico

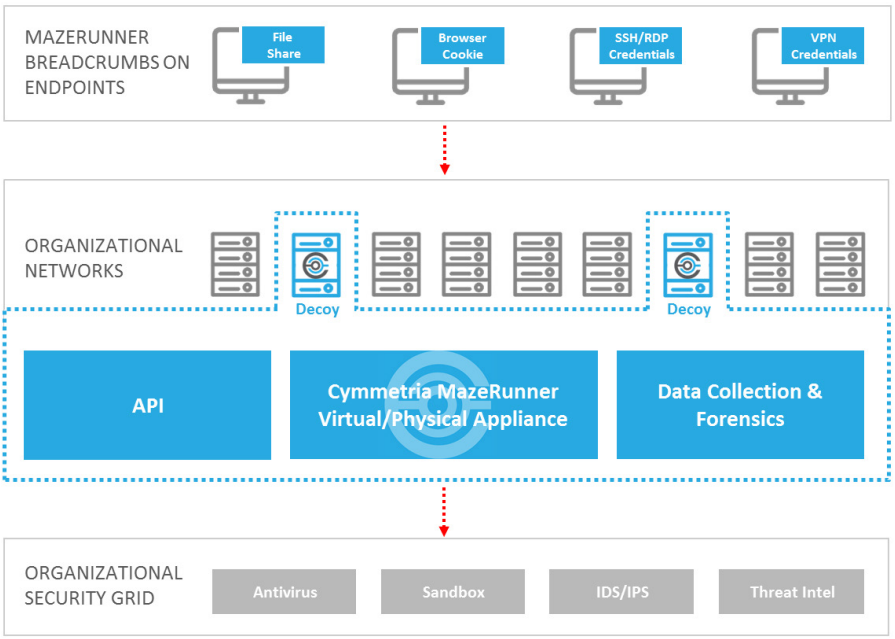
Intercetta gli attaccanti durante la fase di ricognizione, quando non hanno ancora conoscenza della rete, e li conduce gli verso un ambiente protetto, approfondendo la natura dell'attacco e comunicando l'alert all'ecosistema di Cyber Defence.

Scalabile e Adattabile

Sfrutta la virtualizzazione per automatizzare la creazione di elementi di inganno, consentendo una distribuzione scalabile a basso impatto. Riduce al minimo gli impatti, integrandosi perfettamente nella rete del cliente ed emulando i suoi processi di business così da rendere ancora più efficace la strategia di inganno.

Migliora dopo ogni Attacco

Monitora il movimento degli attaccanti fin dall'inizio, raccogliendo preziose informazioni su strumenti, tattiche, approccio vettoriale e comportamento. Una volta che l'attacco viene isolato nell'ambiente controllato, sarà più facile mantenere traccia di tutte le azioni effettuate dall'attaccante, consentendo una più rapida ed efficace analisi forense. Ogni attacco monitorato espande la conoscenza rispetto al "nemico" e questo aiuta a reagire più velocemente alle minacce.



CARATTERISTICHE UNICHE

Gli attacchi sono sempre più dinamici e quindi per affrontarli è necessaria una soluzione dinamica. La **Cyber Deception** è una strategia che trasforma l'attuale asimmetria della Cyber Security, tutta a vantaggio degli attaccanti, consentendo ai difensori di prendere il soppravvento.

La soluzione **Cymmetria MazeRunner**, è una soluzione dinamica, che può aiutare le organizzazioni a difendere le proprie risorse critiche dalle minacce Cyber. È completamente personalizzabile e facilmente implementabile, non appesantisce la rete e potenzia l'efficacia del team di Cyber Defence.

L'unicità della soluzione **Cymmetria MazeRunner**, è data da alcune importanti caratteristiche:

- **Allarmi e avvisi tempestivi**
  Una volta che gli aggressori cadono nell'inganno, vengono generati avvisi in tempo reale. Gli avvisi vengono generati non appena gli aggressori tentano di utilizzare credenziali rubate in qualsiasi punto della rete si trovino.
- **Semplice implementazione**
  Si tratta di una tecnologia che non produce impatti significativi sull'organizzazione, integrandosi perfettamente nella rete e simulando i processi aziendali.
- **Automatizza il processo decisionale**
  L'implementazione segue logiche dinamiche per cui la strategia di inganno viene implementata dove è necessario e quando è necessario.

gruppo Daman
Passione e Innovazione

La soluzione Cymmetria MazeRunner è distribuita in Italia dal Gruppo Daman.

Per saperne di più:
www.gruppodaman.it

Per contattarci:
comunicazione@gruppodaman.it
+39.800.741.423

PREVENIRE E INDIVIDUARE GLI ATTACCHI

Cymmetria offre una strategia basata sull'inganno per monitorare il movimento degli attaccanti fin dall'inizio, raccogliendo preziose informazioni su strumenti e tattiche utilizzate, sull'approccio vettoriale e sul comportamento