CYBER DECEPTION

Cymmetria - MazeRunner

la strategia dell'inganno per fermare il Cyber Crime

MazeRunner, di Cymmetria, usa una strategia di deception, e quindi una strategia basata sull'inganno, per organizzare la difesa dagli attacchi Cyber. Il fattore chiave di uesta strategia consiste nell'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 necessarie contromisure per neturalizzarla.

La strategia adottata da MazeRunner si basa sul principio che la maggior parte degli attacchi segue uno schema prevedibile:

- 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.

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, MazeRunner agisce per facilitare la neutralizzazione della minaccia, comunicando con l'architettura di difesa esistente ed esportando le informazioni sulla minaccia così da creare un impronta dell'attacco.

LA STRATEGIA DI DIFESA

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

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

ARCHITETTURA

L'architettura di MazeRunner è basata su appliance fisiche e virtuali, che sono costituite dai seguenti elementi:

- Un'interfaccia centrale di gestione basata su web.
- Breadcumbs - elementi passivi (agentless) che contengono dati "attrattivi" per un attaccante (es.Cookie, RDP e SSH, credenziali, 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, MazeRunner attiva il processo di notifica e la raccolta di informazioni di dettaglio.
- Componenti che favoriscono l'integrazione con i tool che costituiscono l'ecosistema di Cyber Security, tra cui il SOC o le soluzioni di Threat Intelligence.

DOMINA IL NEMICO

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

SOLUZIONE SCALABILE E ADATTABILE

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

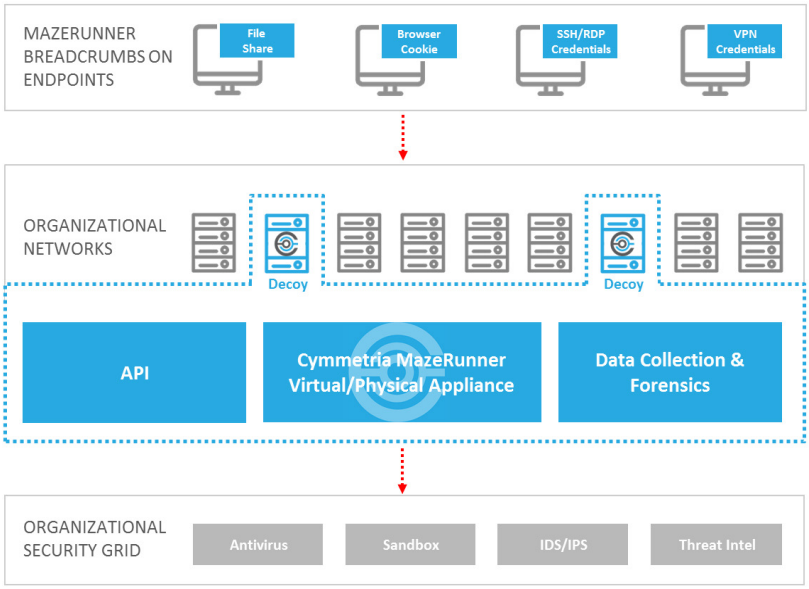
MIGLIORA DOPO OGNI ATTACCO

Cymmetria monitora il movimento degli attaccanti fin dall'inizio, raccogliendo preziose informazioni su strumenti, tattiche, approccio vettoriale e comportamento. Una volta 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.

CONCLUSIONI

Gli attacchi sono dinamici e quindi per affrontarli è necessaria una soluzione dinamica. La Cyber Deception trasforma l'attuale asimmetria della Cyber Security, 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.



GRUPPO DAMAN

La soluzione Cymmetria MazeRunner è distribuita in Italia dal Gruppo Daman, una realtà che ha come principale obiettivo quello di aiutare le grandi organizzazioni, sia pubbliche che private, a massimizzare il valore di business delle proprie infrastrutture tecnologiche.

Questo obiettivo viene perseguito attraverso la distribuzione di tecnologie innovative, accuratamente selezionate sul mercato internazionale, e la loro trasformazione in soluzioni in grado soddisfare le peculiari esigenze delle aziende italiane.

Tra le aree di intervento del Gruppo Daman, la più strategica è quella della Cyber Security, caratterizzata da un elevato livello di specializzazione e da soluzioni tecnologiche allineate con le nuove metodologie di Cyber Defence. In quest'area il Gruppo Daman si avvale di una collaborazione sinergica con la società israeliana Cyber Security Group, insieme alla quale ha dato vita anche a Cyber Academy Italia, considerato un centro di formazione di eccellenza.

Per saperne di più: www.daman.it

Per contattarci: info@daman.it - +39.06.5159281