DECEPTIVE BYTES

Active Endpoint Cyber Defense

Prevention by Deception

Battere i cattivi sul loro campo di battaglia

Il 98% dei malware usa almeno una tecnica di evasione sandbox". Il malware è molto intelligente ed evasivo, utilizzando diverse tecniche per eludere il rilevamento e l'analisi da parte di sistemi di sicurezza classici.
Deceptive Bytes fornisce una soluzione innovativa contro le minacce nelle risorse più critiche ed esposte delle imprese, gli endpoint! **La soluzione crea informazioni dinamiche e ingannevoli** che interferiscono con qualsiasi tentativo di ricognizione dell'ambiente e **dissuadono l'attaccante dall'eseguire ogni attacco**, assicurandosi costantemente che endpoint e dati nell'azienda sono protetti.

Difesa Preventiva

Induce a credere al malware che è in un ambiente poco attraente ed ostile da attaccare, riducendo la motivazione del malware all'attacco e la possibilità di infezione. Ad esempio: la creazione di un ambiente sandbox di detonazione che scoraggia il malware.

Difesa Proativa

Risponde dinamicamente alle minacce man mano che si evolvono, in base all'attuale fase di attacco ed alla modifica del risultato dell'attacco. Ad esempio: ingannando e arrestando Ransomware, ritenendo che sia riuscito a crittografare i file, invece la soluzione li protegge.

Gartner
COOL VENDOR 2019

"Una delle startup più promettenti nella sicurezza informatica"
CBINSIGHTS

Aiutiamo

Organizzazioni

Protegge da minacce sconosciute e sofisticate.
Previene danni a dati e risorse.
Riduce il rischio reputazionale.
Riduce il carico operativo.

CISOs/IT Managers

Automatizza le risposte contro i malware rilevati.
Riduce avvisi e falsi positivi.
Si adatta ai cambiamenti negli ambienti IT.
Utilizza gli strumenti di sicurezza integrati di Windows: Defender e Firewall.
Opera in ambienti senza patch.

C Level

Migliora la produttività dei dipendenti.
Riduce i costi e le risorse operative.
Protegge i dipendenti remoti.

Contatti

company@deceptivebytes.com

Seguici

Situazione attuale

Un milione di nuovi malware viene creato ogni giorno per spionaggio, furto, riscatto e altro, causando danni in miliardi di dollari.

I CISO e i responsabili IT sono sopraffatti da implementazioni complesse e costose di prodotti per la sicurezza degli endpoint, da avvisi e informazioni sugli attacchi e da troppi falsi positivi (F/P). Resta inteso che non sono in grado di gestire tutti gli allarmi e sono gravosi di gestire tali prodotti, ritardando nel fornire i tempi di risposta adeguati e risolvendo i problemi sollevati da vari attacchi.

Ecco come Deceptive Byte aiuta ad affrontare questi problemi con la sua **tecnologia ad inganno**.

Risponde dinamicamente alle minacce mentre si evolvono e protegge sull'intera Endpoint Kill Chain!

Preventivo e Proattivo

Previene minacce sconosciute e sofisticate

Utilizza comportamenti comuni ai malware e previene le minacce in modalita signatureless.

Tassi di prevenzione e rilevazione molto elevati

Oltre il 98% di tutti i malware utilizza tecniche di evasione. L'utilizzo di queste tecniche contro i malware stessi aiuta ad aumentare sostanzialmente i tassi di prevenzione e rilevamento.

Rilevazione e risposta in tempo reale

La soluzione identifica il comportamento dannoso durante l'esecuzione anche se non è stata utilizzata alcuna tecnica di evasione, bloccandola in tempo reale.

Leggero

Protezione a livello di sistema con gestione puntuale

Non ha bisogno di scansionare tutto, gestisce solo processi sconosciuti.

Si distribuisce in pochi secondi

L'agente thin (<1,5 MB) si distribuisce in pochi secondi e funziona istantaneamente senza riavviamento.

Facile da usare

Funziona automaticamente e non richiede un intervento costante, il che rende il consumo di risorse estremamente basso.

Consumo di risorse estremamente basso (CPU, memoria, memoria)

Non influisce sull'esperienza utente e utilizza <0,01% di CPU, <20 MB di memoria e <1,5 MB di spazio su disco.

Senza firma

Nessun aggiornamento costante

Non è necessario aggiornare frequentemente il SW poiché utilizza schemi comportamentali comuni ai malware.

Può funzionare da solo

Nessun aggiornamento periodico significa che la soluzione può funzionare in ambienti isolati, o per dipendenti remoti.

Blocca milioni di minacce usando solo 1 tecnica di evasione

L'integrazione di una tecnica di evasione può potenzialmente bloccare milioni di malware che usano la stessa tecnica, anche quelli futuri.

Affidabilità

Alta stabilità: funziona in modalità utente

L'agente thin funziona in modalità utente, il che significa che non può causare guasti al sistema o utilizzato come punto di accesso a potenziali aggressori e ottenere pieno accesso al sistema operativo.

Autorizza automaticamente i processi legittimi

La soluzione autorizza automaticamente i processi del sistema operativo e altre soluzioni di sicurezza.

Tasso di falsi positivi da basso a inesistente

La soluzione crea vari ambienti contro comportamenti dannosi, attivando avvisi ad alta fedeltà e riducendo il tasso di F/P vicino a zero.