Traps: protezione avanzata per gli endpoint

TRAPS:

- Impedisce tutti gli exploit delle vulnerabilità
- Impedisce tutti gli attacchi malware-driven
- Fornisce informazioni forensi immediate sugli attacchi bloccati
- È scalabile, leggero e facile da usare
- Si integra con le funzioni di sicurezza di rete e cloud

Traps di Palo Alto Networks® fornisce protezione avanzata per gli endpoint, in grado di bloccare exploit di vulnerabilità sofisticati e attacchi malware. A tale scopo, Traps sfrutta un agente altamente scalabile e leggero, che utilizza un nuovo approccio innovativo per gestire gli attacchi senza richiedere alcuna conoscenza preliminare della minaccia. In questo modo, Traps offre alle aziende uno strumento sofisticato per proteggere gli endpoint praticamente da qualsiasi attacco mirato.

Traps di Palo Alto Networks applica un approccio unico alla sicurezza degli endpoint, pensato per offrire una protezione completa, con prevenzione degli attacchi convenzionali così come avanzati e mirati, che le soluzioni tradizionali non riescono a impedire.

Anziché tentare di identificare milioni di singoli attacchi, o di rilevare comportamenti dannosi che possono risultare non tracciabili, Traps si concentra sulla sequenza di tecniche di base che l'autore di qualsiasi attacco deve necessariamente seguire. Inserendo nel processo una serie di "trappole" per gli exploit, finalizzate a mitigare queste tecniche, Traps è in grado di contrastare l'attacco immediatamente, prima dell'esecuzione di qualsiasi attività dannosa.

Questo approccio assolutamente unico consente a Traps di essere agnostico rispetto all'applicazione, proteggendo tutte le applicazioni, incluse quelle elaborate da terze parti.

Prevenzione degli exploit

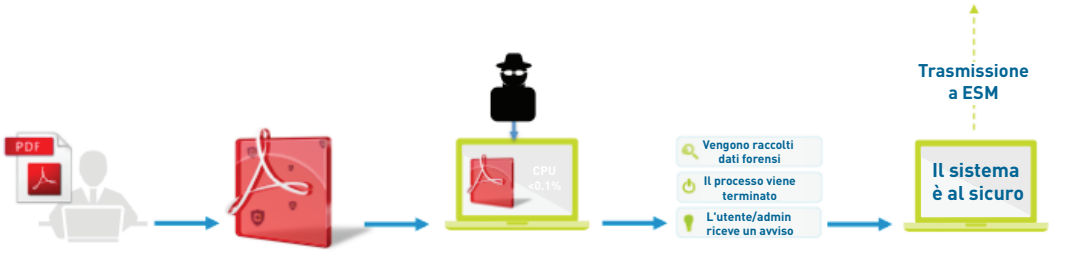
Il processo effettivo di exploit di una vulnerabilità su un endpoint richiede l'esecuzione di diverse tecniche avanzate che operano in sequenza. Ad esempio, nel corso di un attacco tipico, l'autore tenterà di ottenere il controllo di un sistema cercando anzitutto di danneggiare o bypassare l'allocazione o gli handler di memoria. Utilizzando tecniche di danneggiamento della memoria, come buffer overflow o danneggiamento dell'heap, l'hacker può sfruttare le debolezze o le vulnerabilità del software target per eseguire un codice specifico. Una volta acquisita la capacità di eseguire il proprio codice, l'autore dell'attacco ha la possibilità di scaricare malware nel sistema o di assumerne il controllo completo.

Indipendentemente dal tipo di attacco o dalla sua complessità, perché l'attacco vada a buon fine, l'autore deve eseguire una serie di tecniche di exploit in sequenza. Anche se il numero di passaggi può variare a seconda degli attacchi, in tutti i casi è necessario impiegare almeno due o tre tecniche finalizzate ad assumere il controllo dell'endpoint di destinazione.

Come funziona la prevenzione degli exploit

Traps utilizza una serie di moduli di prevenzione exploit concepiti per mitigare e bloccare le diverse tecniche di exploit esistenti. Questi moduli funzionano come "trappole", integrate nei processi utente e progettate per attivarsi e bloccare immediatamente il tentativo di esecuzione della tecnica di exploit da parte dell'autore dell'attacco. A ogni apertura di un'applicazione, Traps inserisce i moduli di prevenzione nel processo, sotto forma di "trappole" statiche. Una volta integrato un modulo, il processo risulta protetto da qualsiasi exploit.

paloalto networks



Come funziona: prevenzione degli exploit.

Se viene eseguito un tentativo di exploit con una delle (poche) tecniche disponibili, Traps blocca immediatamente la tecnica specifica, termina il processo e avvisa l'utente e l'amministratore dell'avvenuto blocco di un attacco. Inoltre, Traps raccoglie dati forensi dettagliati e li comunica all'Endpoint Security Manager (ESM). Data la natura concatenata degli exploit, è sufficiente bloccare una sola tecnica della sequenza per impedire l'intero attacco.

Se non viene compiuto alcun tentativo, tutto procede normalmente, per l'utente e per il processo. Dato l'utilizzo minimo delle risorse da parte di Traps, le misure preventive implementate dietro le quinte non influenzano l'esperienza dell'utente.

Concentrando l'attenzione sulle tecniche di exploit, anziché sull'attacco, Traps può prevenire l'attacco senza conoscere preventivamente la vulnerabilità, a prescindere dalle patch applicate e senza necessità di firme o aggiornamenti software. È importante notare che Traps non esegue attività di scansione o monitoraggio delle attività sospette: il suo approccio presenta quindi un vantaggio enorme in termini di scalabilità, data la quantità limitata di CPU e di memoria utilizzata.

La prevenzione degli exploit di Traps è progettata per prevenire gli attacchi contro le vulnerabilità dei programmi basate sul danneggiamento della memoria o sui difetti logici. Seguono alcuni esempi di attacchi che Traps è in grado di impedire:

- Danneggiamento della memoria
- Esecuzione di codice Java nei browser, in determinate condizioni
- Diffusione indiscriminata di processi figlio da parte di file eseguibili, in determinate condizioni
- Hijacking delle DLL (sostituzione di una DLL legittima con una dannosa avente lo stesso nome)
- Hijacking del flusso di controllo di programma
- Inserimento di codice dannoso sotto forma di exception handler

Prevenzione antimalware

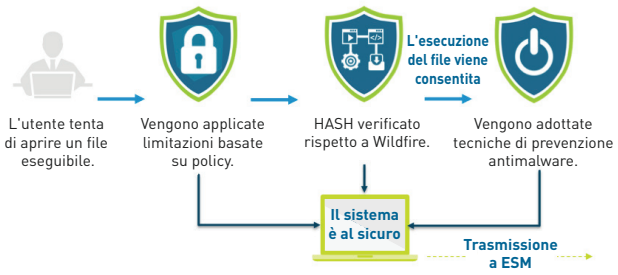
File eseguibili dannosi, noti come malware, sono spesso mascherati o incorporati in file non dannosi. Questi file possono danneggiare i computer nel tentativo di assumerne il controllo, raccogliere informazioni sensibili o interrompere il normale funzionamento del sistema.

Mentre gli autori di attacchi avanzati tendono sempre più a sfruttare le vulnerabilità del software, stanno aumentando anche gli attacchi mediante malware sconosciuti o manipolati (file eseguibili); inoltre, poiché a questi tipi di attacchi in genere non sono associati firme, stringhe o comportamenti già noti, gli approcci di sicurezza endpoint tradizionali non sono in grado di prevenirli.

Per prevenire efficacemente l'esecuzione di malware nel computer, Traps si avvale dei tre componenti seguenti per la prevenzione antimalware:

1. **Limitazioni basate su policy:** le limitazioni basate su policy forniscono alle organizzazioni la possibilità di impostare policy che limitano determinati scenari di esecuzione, anziché adottare white list o black list per file specifici. La superficie di attacco può essere ridotta in modo significativo controllando semplicemente l'origine dell'installazione del file. Quando un utente tenta di aprire il file eseguibile, Traps valuta le regole potenzialmente applicabili che ne limitano l'esecuzione. Esempi di limitazioni comuni basate su policy:
   - Esecuzione di file eseguibili da determinate cartelle
   - Esecuzione di file eseguibili da supporti esterni
   - Generazione di processi figlio da parte di processi padre
   - Esecuzione di processi Java dal browser
   - Esecuzione di processi non firmati
   - Thread injection
2. **Verifica tramite Wildfire™:** per l'esecuzione di file privi di limitazioni attive basate su policy, Traps Endpoint Security Manager interroga il cloud di WildFire sulle minacce mediante un hash, per determinare se il file è dannoso, benigno o sconosciuto all'interno della community globale delle minacce. Se WildFire conferma che un file è un malware noto, Traps ne impedisce l'esecuzione e informa l'ESM.

3. **Mitigazione delle tecniche malware:** come per le tecniche exploit, gli autori di questo tipo di attacchi utilizzano tecniche identificabili e comuni, nel tentativo di distribuire il malware. Nel caso in cui l'esecuzione del file non sia limitata da una policy o non venga associata tramite hash a un attacco noto nel cloud delle minacce di Wildfire, Traps implementa misure di mitigazione basate su tecniche per limitare o bloccare elementi come processi figli, processi Java avviati all'interno di browser web, creazione di thread e processi remoti ed esecuzione di processi non firmati, il tutto per impedire completamente l'esecuzione dell'attacco.



Come funziona: prevenzione antimalware.

Indagini forensi

Ogni volta che Traps impedisce un attacco, vengono raccolte informazioni forensi dettagliate in tempo reale sull'evento in relazione a: file, eventi verificatisi, stato della memoria al momento del blocco dell'attacco e così via. Le informazioni registrate vengono quindi trasmesse all'Endpoint Security Manager (ESM). Anche ad attacco bloccato, rimane disponibile una quantità notevole di intelligence che è possibile acquisire. Acquisendo tutti i dati forensi relativi al tentativo di attacco, le organizzazioni possono applicare difese proattive ad altri endpoint potenzialmente non protetti.

Architettura di Traps

Traps fornisce una struttura di gestione a 3 livelli, costituita da Manager Endpoint Security, Endpoint Connection Server e dagli agenti endpoint. Questo modello rende possibile una significativa scalabilità orizzontale, pur mantenendo configurazione e database centralizzati per policy, dati forensi e così via.

Endpoint Security Manager

Endpoint Security Manager fornisce una dashboard di amministrazione per la gestione degli eventi di sicurezza, dello stato di integrità degli endpoint e delle regole di policy. ESM gestisce anche la comunicazione con Wildfire, in caso di trasmissione di hash a scopo di verifica. Il centro di gestione unificato di ESM comprende:

- Gestione delle configurazioni
- Registrazione e query di database
- Dashboard di amministrazione e panoramica sulla sicurezza
- Acquisizione di dati forensi
- Configurazione di integrazione

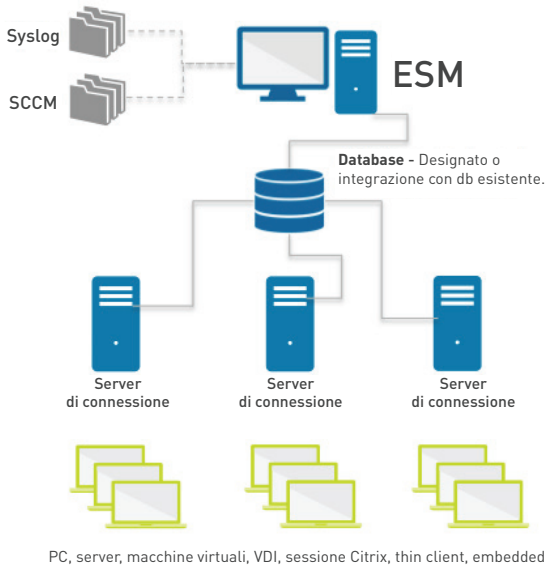
Endpoint Security Manager include un database centralizzato che memorizza informazioni amministrative, regole delle policy di sicurezza, cronologia degli endpoint e altre informazioni sugli eventi di sicurezza. Il database è gestito sulla piattaforma MS-SQL.

Endpoint Security Manager è in grado di scrivere log su una piattaforma di registrazione esterna, ad esempio SIEM, SOC o syslog, oltre a memorizzare internamente i propri registri. Specificando una piattaforma di registrazione esterna è possibile ottenere una visualizzazione aggregata dei registri da tutti gli Endpoint Server.

Endpoint Server

L'Endpoint Server distribuisce regolarmente la policy di sicurezza a tutti gli agenti e gestisce tutte le informazioni relative agli eventi di sicurezza.

- **Stato Traps:** avvisi e pagine di stato in Endpoint Security Manager mostrano le condizioni di ciascun endpoint.
- **Notifiche:** l'agente di Traps invia messaggi di notifica all'Endpoint Server in relazione alle modifiche intervenute sull'agente (ad esempio avvio o arresto di un servizio).
- **Report sulla prevenzione:** Traps riferisce tutte le informazioni relative a un evento all'Endpoint Server, in tempo reale.



Copertura e piattaforme supportate

Traps protegge i sistemi privi di patch, non richiede hardware, ed è supportato su qualsiasi piattaforma in cui viene eseguito Microsoft Windows; desktop, server, sistemi di controllo industriali, terminali, VDI, macchine virtuali, sistemi embedded e così via.

Traps supporta attualmente i seguenti sistemi operativi Windows:

WORKSTATION

- Windows XP SP3
- Windows 7
- Windows 8.1
- Windows Vista SP1

SERVER

- Windows Server 2003
- Windows Server 2008 (+R2)
- Windows Server 2012 (+R2)

Specifiche

Con il suo approccio esclusivo, Traps opera in modo statico, senza eseguire scansioni alla ricerca di attività dannose; il suo utilizzo delle risorse è quindi estremamente limitato:

AGENTE TRAPS:

- CPU: utilizzo medio dello 0,1%
- Consumo di memoria: 25 MB
- Spazio su disco: 15 MB

paloalto networks®
the enterprise security company™

4401 Great America Parkway
Santa Clara, CA 95054

Telefono: +1.408.753.4000
Vendite: +1.866.320.4788
Assistenza: +1.866.898.9087

www.paloaltonetworks.com