SONICWALL

CINQUE PUNTI DEBOLI DELLE ATTUALI SOLUZIONI SANDBOX

Cosa occorre sapere per essere sempre un passo avanti rispetto alle minacce persistenti avanzate

Una minaccia persistente avanzata (Advanced Persistent Threat, APT) è un insieme di processi di pirateria informatica occulti e continui, spesso orchestrati da criminali che prendono di mira un'entità specifica. In molti casi queste minacce includono malware sconosciuti e non ancora documentati, tra cui le minacce zero-day. Sono progettate per essere dinamiche, polimorfiche e in continua evoluzione e hanno lo scopo di sottrarre o compromettere dati sensibili come le informazioni relative a identità, accesso e controllo. Pur essendo meno comuni rispetto alle minacce automatizzate o standardizzate, create per colpire un ampio spettro di obiettivi, gli attacchi APT rappresentano un grave rischio.

Per rilevare più efficacemente le minacce persistenti avanzate, i professionisti della sicurezza stanno mettendo in campo tecnologie di rilevamento avanzate, spesso dotate di sandbox virtuali che analizzano il comportamento di file sospetti e consentono di identificare malware nascosti e non ancora conosciuti. Tuttavia le minacce si fanno sempre più subdole e intelligenti e molte tecniche di sandboxing in commercio non hanno tenuto il passo. In questo articolo esaminiamo cinque aspetti che riducono l'efficacia delle tradizionali tecniche di sandboxing e analizziamo ciò che serve a un'azienda per tenere testa alle minacce persistenti avanzate.

Le attuali tecnologie di rilevamento delle minacce avanzate spesso segnalano solo la presenza e il comportamento dei malware.

1. Infiltrazione delle minacce prima dell'analisi

Innanzitutto, alcune soluzioni di sandboxing non forniscono un giudizio di analisi fino a quando un file potenzialmente pericoloso non è già penetrato nel perimetro della rete. Ciò aumenta i possibili vettori a disposizione di un file dannoso per infiltrarsi nella rete oltrepassandone il perimetro.

2. Analisi limitata dei file

In secondo luogo, alcune soluzioni di sandboxing basate sul gateway presentano limiti per quanto riguarda la dimensione e la tipologia dei file o gli ambienti operativi che riescono ad analizzare. In molti casi sono in grado di identificare solo minacce che sono mirate a un unico ambiente informatico, mentre al giorno d'oggi le aziende lavorano con più sistemi operativi, tra cui Windows, Android e Mac OS X.

La maggiore diffusione di dispositivi mobili e connessi ha inoltre ampliato il campo d'azione delle minacce. Nel 2015, Dell SonicWALL ha rilevato una grande varietà di nuove tecniche offensive e difensive per aumentare la forza degli attacchi contro l'ecosistema Android, presente in quasi l'85% degli smartphone al mondo. Le attuali tecnologie di rilevamento delle minacce avanzate spesso analizzano e rilevano solo le minacce dirette a sistemi operativi e applicazioni di produttività aziendale tradizionali, lasciando così le organizzazioni esposte agli attacchi concepiti per colpire i moderni ambienti di dispositivi mobili e connessi.

Inoltre, alcune di queste tecnologie non sono in grado di analizzare un'ampia gamma di file aziendali standard, tra cui programmi eseguibili (PE), DLL, PDF, documenti di MS Office, archivi, file JAR e APK. A causa di questi limiti, le minacce zero-day sconosciute possono infiltrarsi nella rete eludendo i sistemi di analisi e identificazione.

3. Motori di sandboxing "a silos"

Le singole soluzioni di sandboxing a motore unico risultano ormai inadeguate.

Ora i malware vengono progettati per rilevare la presenza di una sandbox virtuale ed eluderla, limitando così l'efficacia delle tecnologie sandbox di prima generazione. Le soluzioni di sandboxing single-engine sono un bersaglio particolarmente facile per le tecniche di evasione.

Inoltre, le tecniche single-engine creano lacune a livello di analisi. L'analisi delle chiamate tra applicazioni e sistemi operativi, ad esempio, può risultare meno granulare rispetto a quella delle chiamate tra hardware e sistemi operativi perché molte di quelle chiamate restano nascoste ai livelli di applicazione.

Una tecnica più efficace consisterebbe nell'integrare livelli di motori di sandboxing multipli. Ciononostante, le soluzioni di sandboxing attuali sono spesso composte da dispositivi single-engine autonomi a silos o da servizi cloud. L'implementazione di più tecnologie di sandboxing, se attuabile, aumenterebbe in modo significativo la complessità di configurazione, l'impegno degli amministratori e i costi.

4. Minacce crittografate

Da molti anni gli istituti finanziari e altre società che trattano informazioni sensibili utilizzano il protocollo HTTPS sicuro, che cripta le informazioni condivise. Ora anche altre piattaforme come Google, Facebook e Twitter stanno adottando questa prassi per effetto di un'esigenza crescente di privacy e sicurezza degli utenti. Sebbene un maggiore utilizzo della crittografia in internet comporti numerosi vantaggi, allo stesso tempo i criminali informatici hanno iniziato a sfruttare questa crittografia come sistema per "nascondere" i malware per evitare che vengano rilevati dai firewall aziendali.

Mediante i protocolli di crittografia SSL (Secure Sockets Layer) e TLS (Transport Layer Security) (SSL/TLS) o il traffico HTTPS, gli hacker più esperti possono cifrare le comunicazioni di comando e controllo e i codici dannosi per eludere i sistemi di prevenzione delle intrusioni (IPS) e di ispezione anti-malware. Questi attacchi possono essere estremamente efficaci, perché gran parte delle aziende non dispone di un'infrastruttura adeguata per rilevarli. Le tradizionali soluzioni di sicurezza per la rete non hanno la capacità di esaminare il traffico SSL/TLS crittografato, oppure le loro prestazioni sono così limitate da renderle inutilizzabili in fase di analisi.

5. Ostacoli a un rimedio efficace

Le attuali tecnologie di rilevamento delle minacce avanzate spesso segnalano solo la presenza e il comportamento dei malware. Anche se la tecnologia di sandboxing identifica in modo efficace una nuova minaccia su un endpoint specifico, le organizzazioni non hanno i mezzi per eliminarla o porvi rimedio. Non dispongono di un metodo semplice ed efficace per far sì che le firme dei firewall vengano aggiornate in una rete globale distribuita.

Una volta scoperto il malware, probabilmente dopo che un sistema ne è rimasto infettato, sarà compito della divisione IT provvedere alle lunghe operazioni per rintracciare il malware, estirparlo e rimediare ai danni ai sistemi che ne sono stati colpiti. Inoltre, l'IT dovrà creare e implementare rapidamente nuove definizioni malware in tutta l'organizzazione per evitare ulteriori attacchi.

Cosa serve

Le tradizionali soluzioni di sandboxing non sono perfette, questo è vero, ma il loro principio di base è solido. Per rendere più efficace la tecnologia di sandboxing occorre dunque eliminarne i difetti. Una soluzione di sandboxing dovrebbe essere almeno in grado di:

- Applicare l'analisi basata su cloud ai file sospetti per rilevare e bloccare le minacce sconosciute all'esterno del gateway finché non viene determinata la loro natura.
- Analizzare una vasta tipologia di file e ambienti operativi, a prescindere dalle dimensioni o dalla crittografia dei file.
- Aggiornare rapidamente e automaticamente le signature di riparazione.
- Integrare più motori di sandboxing per contrastare meglio le tattiche di elusione, acquisire maggiore visibilità sui comportamenti malevoli e migliorare la capacità di rilevamento delle minacce.
- Ridurre i costi e la complessità.

Scopri di più.

Scopri perché una soluzione sandboxing multilivello rileva più minacce zero-day. Guarda il webcast on demand.

> Una tecnica più efficace consisterebbe nell'integrare livelli di motori di sandboxing multipli.

Informazioni su SonicWall

Da oltre 25 anni SonicWall combatte il crimine informatico, proteggendo piccole, medie e grandi imprese in ogni parte del mondo. La nostra combinazione di prodotti e partner ha permesso di realizzare una soluzione di difesa informatica in tempo reale ottimizzata per le specifiche esigenze di oltre 500.000 aziende internazionali in più di 150 paesi, per consentire loro di fare più affari con maggior sicurezza.

Per qualsiasi domanda sul possibile utilizzo di questo materiale, contattare:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com