N-ABLE™

Antivirus e soluzioni di rilevamento risposta per gli endpoint

Cosa c’è da sapere

E-book

Introduzione

L'obiettivo dei clienti è proteggere reti e utenti finali. Qual è la migliore difesa? Una soluzione di sicurezza su più livelli, come gli strati di una cipolla, che però - a differenza della cipolla - ti faranno evitare le lacrime. Gli antivirus e le soluzioni di rilevamento e risposta per gli endpoint contribuiscono a garantire la sicurezza del software dei clienti, ma lo fanno in modi differenti.

Come fai a sapere qual è l'approccio giusto per te? Le soluzioni di rilevamento e riposta per gli endpoint soppianteranno definitivamente gli antivirus?
Niente panico: le risposte a entrambe le domande sono semplici. Continua a leggere per scoprirle.

ANTIVIRUS

Una protezione adeguata, ma solo se aggiornata

In parole semplici, gli antivirus proteggono i clienti dal malware e ti aiutano ad aggiornare i programmi automatici e le definizioni dei virus, così non dovranno farlo i clienti. Eventuali malware o virus rilevati vengono automaticamente messi in quarantena. Ecco perché gli antivirus hanno rappresentato per anni lo standard della sicurezza e perché i clienti ne sono esperti.

Ma questa procedura ha un rovescio della medaglia. Se da un lato gli antivirus proteggono da virus e software dannosi, questi rappresentano solo una piccola parte delle tante minacce ai danni degli endpoint. E, nonostante gli antivirus occupino ancora una posizione prominente, essi richiedono il regolare aggiornamento delle definizioni (firme) dei virus. Questo significa che gli antivirus dei clienti offrono una protezione adeguata solo se sono dotati degli aggiornamenti più recenti; inoltre, i furbi criminali informatici di frequente impiegano tecniche di evasione per eludere anche software aggiornati. Purtroppo, la maggioranza delle minacce che sfuggono agli antivirus vengono identificate soltanto dopo che il danno è stato fatto.

Di seguito, vengono illustrate cinque tipologie di attacchi che si avvalgono di tecniche di evasione.
Continua a leggere per comprendere al meglio con cosa hai a che fare.

Cinque tecniche di attacco elusive in grado di sfuggire ai controlli degli antivirus

1 Malware polimorfi

Anche se utili, i programmi antivirus potrebbero non garantire la sicurezza necessaria, come invece si potrebbe pensare. Molti programmi antivirus tradizionali si affidano massicciamente al rilevamento basato su firme, vale a dire che essi confrontano un file rispetto a una nuova voce (o firma) presente in un database di minacce note (ripetiamolo, "note").

Per funzionare correttamente l'utente dell'antivirus necessita delle più recenti firme, il che richiede aggiornamenti frequenti. Ma se le definizioni dei virus non vengono aggiornate, di fatto l'utente risulta privo di difese rispetto ai nuovi file. Ecco perché è fondamentale che le aziende antivirus vengano a conoscenza della firma prima che possano distribuirla alla propria base utenti. I criminali informatici conoscono questa procedura ed è per questo che creano malware in grado di eludere il rilevamento degli antivirus.

Uno dei preferiti tra gli hacker? Il malware polimorfo. Si tratta di un metodo specificamente concepito per sfruttare queste falle degli antivirus. Anche solo una piccola falla nella copertura può creare danni. Poniamo che il tuo programma antivirus rilevi la presenza di malware. Ottimo, no? Sì, ma purtroppo l'attacco continuerà a rigenerarsi utilizzando nuove caratteristiche che di proposito non corrispondono alle firme cui si affida l'antivirus. L'infezione purtroppo è in corso.

2 Documenti utilizzati per sferrare un attacco

I criminali informatici preferiscono adottare un approccio lento e graduale per giungere all'obiettivo, così utilizzano i tuoi documenti come armi contro di te manipolandone il codice (script). È una tipologia di attacco furtivo, non rapido, che avviene in background senza che l'utente se ne accorga.

I criminali informatici possono utilizzare documenti quali file PDF di Adobe® con codice JavaScript® incorporato per eseguire comandi del sistema operativo o scaricare file eseguibili per compromettere i dispositivi e le reti a cui accedono.

Potrebbero inoltre impiegare script incorporati per eseguire comandi PowerShell®. Questo è importante perché tali comandi sono integrati nel sistema operativo Windows® e possono diffondersi non solo negli endpoint, ma in intere reti. Tali tattiche potrebbero esporre anche i documenti XML, HTML e Office® ed eludere le soluzioni antivirus che mettono a confronto le firme eseguibili. Una soluzione antivirus analizza solo il documento iniziale, non il codice dannoso avviato dal documento stesso.

3 Download drive-by tramite browser

Hai mai avviato un download dal browser e assistito poi a una serie di download successivi? I criminali informatici li sfruttano a proprio vantaggio. Si tratta dei cosiddetti "download drive-by", una tattica che prevede il download di file dannosi sull'endpoint mediante lo sfruttamento delle vulnerabilità del browser. Purtroppo in questo caso non basta evitare i siti sospetti, perché anche quelli legittimi potrebbero comunque avere uno script compromesso o un servizio pubblicitario. Tali download possono provenire da qualsiasi canale (e-mail, phishing sui social o link pop-up nascosti), in grado di attrarre gli utenti verso un sito web. Quando i criminali informatici riescono a eludere le difese, sfruttano gli exploit di browser o plug-in per scaricare malware e sferrare l'attacco.

4 Attacchi senza file

Gli antivirus necessitano di file da ispezionare per tenere i sistemi al sicuro. E se non ci fosse alcun file da rilevare? I criminali informatici possono impiegare gli attacchi senza file per eludere gli antivirus senza essere scoperti. Pazzesco, vero? E non hanno neanche bisogno di installare un payload su un sistema. Tali attacchi possono diffondersi nella memoria degli endpoint utilizzando PowerShell, rundll32.exe o altri sistemi incorporati.

Ma queste minacce senza file hanno altri assi nella manica da sfruttare. Ad esempio, quando il computer impiega il Remote Desktop Protocol, apre una porta di ascolto sulla macchina che consente ai malintenzionati di connettervisi. Quindi gli hacker possono eseguire processi dannosi come scaricare malware basati su file reali, apportare modifiche al registro o impadronirsi dei dati.

5 Malware offuscato

Le aziende antivirus dispongono di diversi metodi per individuare i malware. Uno di questi comporta l'esecuzione di file in ambienti sandbox e l'osservazione di eventuali comportamenti sospetti. Un altro diffuso metodo di individuazione consiste nella scansione del codice per cercare segnali che comunemente indicano un intento criminoso.

Ma i criminali informatici hanno scoperto stratagemmi per evitare tutto questo. Così come i professionisti della sicurezza proteggono i propri asset, anche gli hacker possono proteggere i payload dannosi presenti nei malware.

I malware più recenti possono persino rilevare la presenza di un ambiente sandbox, dove non risultano dannosi, per poi sferrare l'attacco nell'ambiente live; successivamente, diventa quasi impossibile che l'antivirus rilevi il malware, quando è integrato nel nuovo ambiente sandbox.

Un altro metodo impiegato dagli hacker per eludere gli antivirus è rappresentato dai cosiddetti packer che impiegano la crittografia o la compressione per impedire agli utenti di notarli. Hai mai somministrato una medicina a un cane inserendola in un pezzo di formaggio? È esattamente questo il trucco. Il codice dannoso può anche essere integrato in codice innocuo per celare i contenuti malevoli.

I criminali informatici sono estremamente furbi, pertanto individuare un attacco nascosto sta diventando sempre più difficile. Talvolta una protezione antivirus può arrecare più danni che benefici. Ad esempio, i programmi antivirus impiegano le scansioni euristiche all'interno di un ambiente sandbox, ma tali tecniche aiutano il malware a sfuggire al rilevamento prima che acceda all'ambiente live della macchina.

SOLUZIONI DI RILEVAMENTO E RISPOSTA PER GLI ENDPOINT

Il futuro della sicurezza degli endpoint

L'idea che i criminali informatici eludano l'antivirus e si insinuino nei sistemi crea ansia in chiunque. Lo sappiamo. Per fortuna, rilevamento e risposta per gli endpoint rappresentano la soluzione che garantisce i vantaggi standard dell'antivirus, offrendo però una sicurezza più avanzata.

Le soluzioni di rilevamento e risposta per gli endpoint non offrono solo la sicurezza avanzata, ma la totale tranquillità. Come nel caso degli antivirus, sono gli MSP che gestiscono queste soluzioni senza che sia necessario alcun intervento da parte degli utenti finali. Le minacce informatiche si diffondono ogni giorno, pertanto gestire diversi endpoint con strumenti tradizionali come gli antivirus può diventare un problema e un rischio per la sicurezza.

Le soluzioni di rilevamento e risposta per gli endpoint rappresentano uno strumento di sicurezza multiuso: non solo si occupano della protezione degli endpoint, ma rilevano un maggior numero di minacce rispetto al solo malware. Insieme al software di monitoraggio e agli agent per gli endpoint, il machine learning integrato e l'intelligenza artificiale avanzata consentono a queste soluzioni di neutralizzare l'attacco prima che arrechi danni. Abbiamo parlato in precedenza degli attacchi senza file. Gli antivirus non sono in grado di rilevarli, a differenza delle soluzioni di rilevamento e risposta per gli endpoint che li studiano con la lente di ingrandimento.

Attività sospette? Anche queste saranno passate al vaglio dalle moderne soluzioni. Poniamo che più file vengano modificati su un endpoint contemporaneamente. Le soluzioni di rilevamento e risposta per gli endpoint possono riconoscere questo comportamento, avvertire l'amministratore e permettergli di bloccarlo. Questi strumenti possono persino rilevare minacce emergenti non ancora scoperte, mentre gli antivirus basati su firme sono totalmente inutili in questi casi.

Molti utenti di antivirus sprecano tempo e risorse con i lenti upload al cloud finalizzati al rilevamento delle minacce. Con gli strumenti di rilevamento e risposta per gli endpoint l'elaborazione avviene invece in locale sull'endpoint, così potrai rilevare rapidamente le minacce e automatizzare il ripristino.

Che succede se il danno è già stato fatto? È necessario scoprire come e perché l'endpoint è stato compromesso. Per fortuna, le soluzioni di rilevamento e risposta per gli endpoint offrono l'analisi attiva delle cause scatenanti, grazie a una cronologia visiva (che somiglia un po' a un album fotografico), da cui è possibile visualizzare il processo che ha dato origine all'attacco, le relative modalità di replica e diffusione e persino la modalità di progettazione della minaccia. In questo modo potrai avvalerti di queste informazioni utili per migliorare la sicurezza dei clienti in futuro.

A seconda della configurazione impostata, la soluzione di rilevamento e risposta per gli endpoint può eliminare, mettere in quarantena ed eseguire il rollback del danno conseguente a un attacco. Potrai, infatti, letteralmente annullare i danni provocati e invalidare gli effetti del ransomware.

Soluzioni antivirus e strumenti di rilevamento e risposta per gli endpoint - Conclusioni

Gli antivirus hanno rappresentato a lungo uno standard per la sicurezza e sono meglio di niente, senza dubbio. Ma le soluzioni di rilevamento e risposta per gli endpoint sono il futuro della sicurezza software e stanno rapidamente diventando il nuovo standard per le seguenti ragioni:

- **Rilevamento proattivo:** le soluzioni di rilevamento e risposta per gli endpoint combinano le funzionalità dell'intelligenza artificiale e del machine learning per rilevare minacce potenziali e colmare le lacune degli antivirus tradizionali.
- **Protezione più ampia:** le soluzioni di rilevamento e risposta per gli endpoint assolvono numerose funzioni. Non solo rilevano virus e malware, ma proteggono anche i clienti da traffico dannoso e attacchi senza file.
- **Indagini rapide sulle minacce:** le soluzioni di rilevamento e risposta per gli endpoint ti aiutano a tornare indietro nel tempo e ad analizzare l'intera catena dell'attività della minaccia in questione, dalla causa scatenante al movimento laterale. Questo offre maggiori informazioni sull'attacco e consente di adeguare le procedure di sicurezza e i controlli per impedire che il problema si verifichi di nuovo.
- **Applicazione rapida di rimedi:** le soluzioni di rilevamento e risposta per gli endpoint consente di eseguire il rollback di un endpoint a uno stato integro precedente all'attacco ransomware direttamente dallo strumento.
- **Ridotto utilizzo delle risorse:** le soluzioni di rilevamento e risposta per gli endpoint consentono di risparmiare tempo e risorse dovuti alle scansioni e agli aggiornamenti ricorrenti. Gli utenti si sentiranno protetti ovunque si trovano mentre lavorano offline.

A questo punto, potresti domandarti perché c'è chi si affida a un antivirus se tutti i criminali informatici hanno capito come eluderlo...

Gli antivirus proteggono gli utenti dalle minacce note, pertanto i tuoi clienti avranno comunque bisogno di supporto nella gestione di tale protezione di base. Tuttavia, la ragione principale per cui gli antivirus sono ancora tanto diffusi risiede nel fatto che hanno un costo per licenza inferiore rispetto alle soluzioni di rilevamento e risposta per gli endpoint. Il prezzo rappresenta sicuramente un aspetto allettante, ma l'utilizzo significativo di risorse e i potenziali svantaggi della protezione antivirus potrebbero alla lunga influire negativamente sulla tua attività. È certo che violazioni come gli attacchi ransomware non saranno trascurate dai clienti potenziali o esistenti. Alla fine, l'investimento in una soluzione di rilevamento e risposta per gli endpoint è più conveniente.

N-able

N-able offre ai provider di servizi IT potenti soluzioni software per monitorare, gestire e mettere in sicurezza sistemi, dati e reti dei relativi clienti. Grazie alla piattaforma scalabile su cui si basano i nostri prodotti, offriamo un'infrastruttura sicura e strumenti adeguati per semplificare ecosistemi complessi e le risorse per stare al passo con le esigenze IT in continua evoluzione. Aiutiamo i nostri partner in ogni fase del loro percorso a proteggere i clienti e a espandere la propria offerta di servizi, grazie a un portafoglio flessibile e in continua crescita di integrazioni fornite dai provider di tecnologie leader del settore. n-able.com/it