
SONICWALL®
Come riconoscere e contrastare gli attacchi informatici
E-BOOK

Introduzione

I moderni criminali informatici hanno perfezionato le loro tecniche già complesse per evitare di essere rilevati quando si introducono furtivamente nelle reti per svariati motivi, che spesso sono di natura puramente economica. Questi cybercriminali cercano di rubare proprietà intellettuale, fare spionaggio, interrompere i processi o esfiltrare file per poi richiedere un riscatto. Utilizzano le tecniche più recenti per eludere il rilevamento, mantenere l'accesso alle reti e svolgere le loro attività dannose senza essere notati.

Una volta trovata una falla, questi criminali provano a scaricare e installare malware nel sistema compromesso. In molti casi, il malware utilizzato è una nuova variante evoluta che i sistemi antivirus non sono ancora in grado di rilevare.

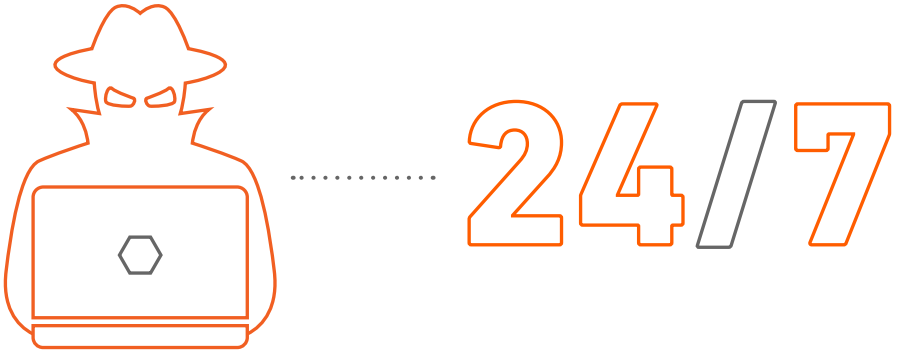
Questo e-book descrive in dettaglio le strategie e gli strumenti usati dai cybercriminali per infiltrarsi nella rete e spiega come contrastare queste strategie per bloccare i criminali informatici sul nascere.

I cybercriminali lavorano senza sosta per sfruttare i punti deboli delle reti.

Strategia di cyber attacco n. 1 Bombardare le reti con malware 24 ore su 24

Il volume totale di malware è in crescita, e alcuni paesi stanno registrando milioni di tentativi di attacco. Gli attacchi per colpire e compromettere una rete possono provenire da ogni tipo di vettore. La posta elettronica, i dispositivi mobili, il traffico web e molto altro sono tutti potenziali obiettivi che gli hacker possono compromettere persino con exploit automatizzati. Le dimensioni dell'azienda presa di mira non contano, a un hacker interessano solo indirizzi IP, indirizzi email o potenziali clienti da sfruttare per un attacco "watering hole". I criminali utilizzano questi strumenti automatizzati per eseguire exploit o per inviare email di phishing 24 ore su 24.

Un problema comune a molte organizzazioni è la mancanza di strumenti adeguati per proteggersi da queste minacce. Molte aziende non dispongono di strumenti automatizzati per ripulire il traffico, proteggere gli endpoint e filtrare le email. Altre utilizzano firewall che non sono in grado di rilevare le minacce nascoste nel traffico crittografato o si affidano a una memoria di sistema integrata limitata per archiviare le firme del malware.



Contrattacco n. 1
Proteggere la rete in ogni momento della giornata

Ogni ora compaiono centinaia di varianti malware mai viste prima; per questo le organizzazioni necessitano di una protezione aggiornata e in tempo reale per contrastare queste nuove minacce. Una soluzione di sicurezza efficace deve disporre delle tecnologie più recenti per rilevare i pericoli in tempo reale e proteggere un'azienda 24 ore al giorno, sette giorni alla settimana. Con un afflusso così massiccio di tipi e varianti di malware, viene superata la capacità di memoria di qualsiasi firewall. Una soluzione che includa servizi di sicurezza come la tecnologia Real-Time Deep Memory Inspection (RTDMI™) rileva e blocca in modo proattivo minacce di massa, zero-day e varianti di malware sconosciute.

Per fornire una visione più ampia possibile del malware e scoprire e identificare le nuove varianti, i firewall dovrebbero utilizzare una sandbox basata sul cloud. Inoltre, è essenziale che la soluzione di sicurezza supporti l'aggiornamento dinamico della protezione non solo per il gateway del firewall, ma anche per gli endpoint mobili e remoti, in quanto i dispositivi IoT (Internet of Things) possono essere sfruttati come punto d'ingresso per eventuali attacchi.

Una piattaforma di sicurezza che sfrutta le potenzialità del cloud per rilevare e prevenire automaticamente le violazioni in tempo reale permette di contrastare i malware più evoluti.

I cybercriminali utilizzano vari tipi di malware per cogliervi alla sprovvista.

Strategia di cyber attacco n. 2 Infettare le reti con diverse forme di malware

I cybercriminali utilizzano diversi vettori di attacco e varianti malware per compromettere le reti. I cinque strumenti più diffusi sono virus, worm, trojan, spyware e ransomware.

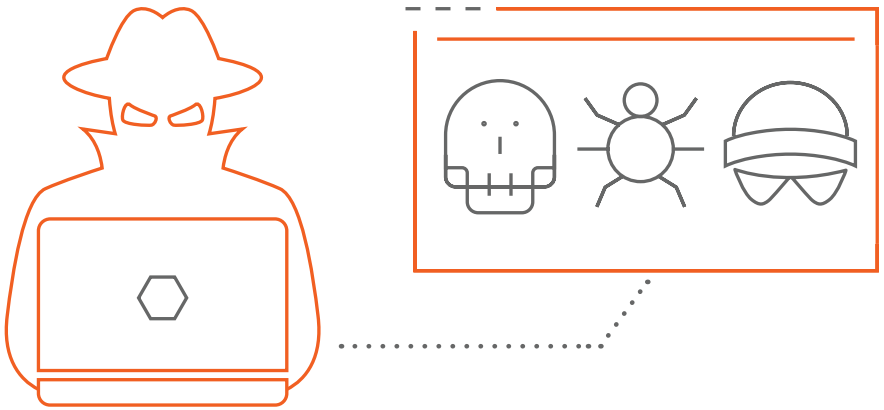
I virus informatici sono stati inizialmente diffusi attraverso la condivisione di supporti infetti. Con lo sviluppo tecnologico, sono via via cambiati anche i metodi di diffusione. Oggi i virus vengono comunemente diffusi attraverso programmi legittimi, condivisione di file, download da Internet e allegati di posta elettronica. Quando vengono aperti o eseguiti, i virus possono commettere una serie di azioni dannose, dalla corruzione dei dati fino al blocco del sistema.

I worm informatici esistono sin dalla fine degli anni '80, ma non hanno avuto particolare importanza fino all'adozione delle infrastrutture di rete all'interno delle aziende. A differenza dei virus, i worm possono autoreplicarsi e propagarsi attraverso la rete senza l'intervento dell'utente. Possono provocare infezioni rapide e sovraccaricare di traffico le reti.

I trojan sono programmi malevoli che si presentano come software o file legittimi e sono appositamente progettati per estrarre dati sensibili dalla rete. Molti tipi di trojan assumono il controllo del sistema infettato e aprono una "porta di servizio" (backdoor) da cui il criminale può accedere al sistema quando meglio crede. I trojan sono spesso utilizzati anche per creare botnet.

Gli spyware non sono dannosi di per sé, ma sono molto fastidiosi perché spesso contagiano i browser web, rendendoli quasi inutilizzabili. Talvolta lo spyware può essere mascherato da applicazione legittima, fornendo all'utente un qualche beneficio ma registrando segretamente quello che viene digitato e la cronologia di navigazione, rubando i dati personali o monitorando i modelli di comportamento e di utilizzo dell'utente. I dati rubati vengono poi inviati all'aggressore, compromettendo la privacy e la sicurezza degli utenti.

Il ransomware è un attacco che spesso cripta i file su un endpoint o su un intero server, rendendoli inaccessibili. I cybercriminali richiedono poi un riscatto, generalmente in bitcoin, che l'organizzazione dovrà pagare per ricevere la chiave di crittografia. Quando il ransomware compromette sistemi business-critical, il costo del riscatto può aumentare fino a diverse centinaia di migliaia di dollari.



Per prevenire gli attacchi è necessaria una protezione su più livelli contro il malware.

Contrattacco n. 2
Assicurarsi che la rete sia protetta contro tutti i tipi di malware

Tutti i firewall dovrebbero proteggere le organizzazioni da ogni tipo di minaccia informatica. Il modo migliore per raggiungere questo obiettivo è integrare tutti i metodi di protezione in un approccio single-pass a latenza ridotta, in modo da bloccare gli attacchi non solo al gateway, ma anche negli endpoint all'esterno del perimetro tradizionale. Una soluzione di sicurezza dovrebbe includere le seguenti funzionalità:

- Protezione anti-malware basata sulla rete per impedire ai criminali di scaricare o trasmettere malware a un sistema compromesso.
- Aggiornamenti continui e tempestivi per proteggere la rete 24 ore su 24 da milioni di nuove varianti malware appena vengono scoperte.
- Servizio di prevenzione delle intrusioni (IPS) per impedire ai criminali di sfruttare le vulnerabilità.
- Sandbox per inviare il codice sospetto a un ambiente isolato nel cloud, dove farlo detonare e analizzare per scoprire malware finora sconosciuto.
- Sicurezza di accesso per applicare contromisure di controllo degli accessi degli utenti presso gli endpoint mobili e remoti, sia all'interno che all'esterno del perimetro di rete.
- Protezione email per bloccare phishing, spam, trojan e attacchi di social engineering trasmessi attraverso la posta elettronica.

La certezza che ogni dispositivo collegato alla rete disponga di un software antivirus aggiornato garantisce una protezione in più contro i malware. Abbinando una soluzione antivirus completa su PC a un firewall, le aziende possono bloccare molti degli strumenti utilizzati dai cybercriminali per compromettere la rete.

Strategia di cyber attacco n. 3
Cercare e compromettere le reti più deboli

Per quanto molti fornitori di firewall si vantino di offrire sistemi di protezione eccellenti, solo in pochi riescono a dimostrare l'efficacia delle proprie soluzioni. Le organizzazioni che utilizzano firewall obsoleti sono erroneamente convinte che la propria rete sia protetta, ma i cybercriminali più esperti sono in grado di aggirare i firewall che non dispongono di misure di sicurezza adeguate, utilizzando algoritmi complessi per eludere i controlli e compromettere la rete.

Alcuni firewall offrono sicurezza a discapito delle prestazioni, per cui le organizzazioni a volte cedono alla tentazione di limitare o disattivare del tutto le misure di sicurezza per non rinunciare ad avere prestazioni di rete elevate. Si tratta di una scelta estremamente rischiosa che andrebbe evitata.

Un'altra vulnerabilità nel sistema di sicurezza della rete è il fattore umano. I criminali contano su potenziali azioni o comportamenti umani che potrebbero compromettere inavvertitamente l'integrità, la riservatezza e la disponibilità di una rete. Le azioni che possono introdurre rischi e indebolire le misure di sicurezza includono truffe di phishing, social engineering, sistemi mal configurati, software non aggiornati, policy di sicurezza ignorate e altro ancora. I cybercriminali sfruttano queste tattiche per ottenere informazioni di accesso e altre autorizzazioni che gli consentano di aggirare le protezioni del firewall e sferrare gli attacchi dall'interno della rete. Inoltre, i dipendenti a volte collegano i loro dispositivi personali alla rete aziendale senza misure di sicurezza adeguate. Ciò può portare ad accessi non autorizzati se un dispositivo personale viene smarrito o lasciato incustodito, esponendo l'azienda a una violazione quando il dispositivo si trova all'esterno del perimetro di sicurezza della rete.

> Spesso i criminali informatici scelgono le loro vittime in base ai punti deboli scoperti nella rete.

> Tutti i firewall necessitano di un motore che protegga la rete dagli attacchi sia interni che esterni, ma senza compromettere le prestazioni.

Contrattacco n. 3
Scegliere una piattaforma di sicurezza completa che offra una protezione eccellente, prestazioni elevate e gestione centralizzata.

Cercate soluzioni di sicurezza con una protezione anti-malware basata sulla rete che sia testata e certificata da società indipendenti.

Le piattaforme multi-core consentono di analizzare file di qualunque tipo e dimensione per gestire flussi di traffico mutevoli. Tutti i firewall necessitano di un motore che protegga la rete dagli attacchi sia interni che esterni senza compromettere le prestazioni.

Cercate un firewall dotato di una sandbox basata su cloud, che può aiutarvi a scoprire nuovi malware mirati specificamente al vostro ambiente. Queste scelte potrebbero fare la differenza tra una normale giornata di lavoro e una in cui i cybercriminali tengono in ostaggio le vostre risorse digitali.

La vostra strategia di sicurezza deve includere la protezione degli endpoint mobili e remoti, sia all'interno che all'esterno del perimetro, per garantire un accesso mobile sicuro.

Inoltre, vi serve una soluzione di protezione delle email per difendervi da phishing, spam, virus, social engineering e altre minacce trasmesse per email. Per formare il vostro personale potete utilizzare il Quiz sul phishing di SonicWall, disponibile gratuitamente.

Strategia di cyber attacco n. 4
Trasformarsi continuamente e sferrare attacchi globali

Molti cybercriminali inventano continuamente nuovi malware e li condividono con altri criminali in tutto il mondo. Questo significa che ogni pochi secondi appaiono nuove minacce in qualsiasi continente. Molti cybercriminali privilegiano il metodo "saccheggio": entrano nella rete, prendono tutto ciò che capita e poi si dileguano prima che venga dato l'allarme. Riescono a entrare e uscire dalla vostra rete prima ancora che ve ne siate accorti. Altri hanno un approccio più lento e prudente, cercando di accedere a una quantità maggiore di dati in un arco di tempo più lungo. Alcuni attacchi arrivano dal web, altri attraverso i messaggi email oppure direttamente dall'interno della rete, a causa di dispositivi che sono stati infettati all'esterno del perimetro di sicurezza della rete.

> Ogni secondo appaiono nuove minacce in tutti i continenti.

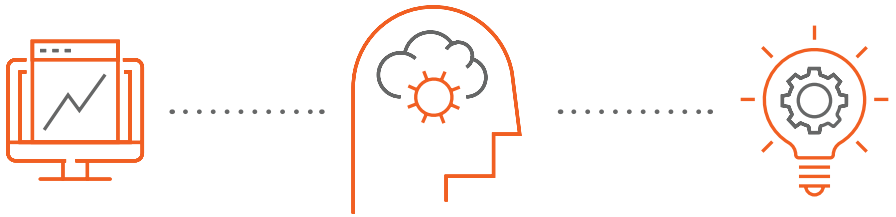
Per bloccare le minacce globali più recenti, occorre investire in una soluzione di sicurezza con intelligence sulle minacce globali.

Contrattacco n. 4 Scegliere un firewall che protegga dalle minacce globali

Una reazione rapida è fondamentale per difendersi al meglio. Per applicare rapidamente delle contromisure alle minacce emergenti, scegliete un fornitore di soluzioni di sicurezza che disponga di un team interno addetto alla threat intelligence, alla ricerca e alla creazione di contromisure. L'ideale è che questo team collabori con l'intera community di esperti in materia di protezione, in modo analogo a come funziona il Rapporto SonicWall sul Cybercrime.

Una soluzione ad ampio spettro utilizza un catalogo completo di malware basato sul cloud per ottimizzare le analisi del firewall locale.

Mentre un semplice firewall si limita a identificare le minacce ed eseguire blocchi in base al criterio dell'area geografica, un firewall di nuova generazione più sofisticato esegue il filtraggio dei botnet e riduce l'esposizione a malware globali noti, bloccando il traffico proveniente da domini pericolosi oppure impedendo la connessione da e verso determinate zone.



Conclusioni

Per sviluppare strategie di difesa efficaci contro gli attacchi informatici basati sulla rete, occorre adottare un approccio olistico che integri pratiche di sicurezza avanzate e l'uso di strumenti di sicurezza efficaci per rilevare e reagire a comportamenti di rete anomali senza compromettere le prestazioni. Rimanendo proattivi, potete adattarvi alle minacce in continua evoluzione e proteggere la vostra organizzazione da pericoli sconosciuti.

Quando siete pronti per valutare una soluzione di contrattacco adatta alle esigenze specifiche della vostra organizzazione, contattate il vostro rappresentante SonicWall o visitateci online per saperne di più sui Next-Generation Firewall (NGFW) di SonicWall.

Per saperne di più ...

Contattaci per richiedere la consulenza di un esperto di sicurezza SonicWall.

Dai un'occhiata alle Live Demo disponibili della nostra linea di prodotti SonicWall.

Visita la nostra pagina web, Firewall di nuova generazione

Guarda una mappa aggiornata degli attacchi in corso nel nostro Capture Labs Security Center.

SONICWALL

SonicWall

SonicWall fornisce soluzioni di cybersecurity innovative per la nuova normalità iperdistribuita, in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e in cui la sicurezza dei dati rappresenta un elemento fondamentale. Con la sua capacità di individuare le minacce più elusive e offrendo una visibilità in tempo reale, SonicWall rende possibili economie innovative e colma le lacune della cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per maggiori informazioni, visitare www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

Ebook-TypesofCyberattacks-JK-8854