SONICWALL®

GLI ATTACCHI INFORMATICI — UNA GUIDA PER RICONOSCERLI ED EVITARLI

Oggigiorno i criminali informatici si servono di una serie di complesse tecniche per evitare di essere identificati mentre si aggirano furtivamente nelle reti aziendali al fine di sottrarne le proprietà intellettuali o di bloccarne i file per poi richiedere un riscatto. Le loro minacce sono spesso crittografate in modo da eludere i controlli.

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.

Il presente e-book illustra in modo dettagliato le strategie e gli strumenti utilizzati dai criminali informatici per introdursi nelle reti e le misure da adottare per bloccarli.

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

Strategia di attacco informatico n. 1

Bombardare le reti con malware 24 ore su 24

Gli attacchi utilizzano ogni possibile veicolo di trasmissione: email, dispositivi portatili, traffico web ed 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.

SONICWALL®

Contrattacco n. 1

Proteggi la rete in ogni momento della giornata

Ogni ora compaiono centinaia di nuove varianti di malware; per questo le organizzazioni devono necessariamente disporre di un metodo di protezione in tempo reale per contrastare anche gli attacchi più recenti. Per essere efficace, una soluzione di sicurezza deve essere aggiornata di continuo, 24 ore al giorno, 7 giorni a settimana. Inoltre, il numero di tipi e varianti di malware è talmente elevato da superare la capacità di memoria di qualsiasi firewall.

Per questo motivo, per avere la più ampia panoramica di tutti i malware, scoprirne le nuove varianti e identificarle nel modo più efficace, è opportuno che i firewall utilizzino una sandbox di rete e il cloud. La soluzione di sicurezza dovrebbe inoltre supportare la protezione ad aggiornamento dinamico non solo per il gateway del firewall ma anche per gli endpoint mobili e remoti e per la posta elettronica.

Avere una piattaforma di sicurezza che sfrutta le potenzialità del cloud significa disporre in tempo reale delle difese contro i malware più evoluti.

Strategia di attacco informatico n. 2

Infettare le reti con diverse forme di malware

I criminali informatici utilizzano vari tipi di vettori di attacco e malware per attaccare le reti, tra cui i cinque più diffusi sono virus, worm, trojan, spyware e ransomware.

I primi virus informatici si diffondevano condividendo floppy disk infetti. Con lo sviluppo tecnologico, sono via via cambiati anche i metodi di diffusione. Oggi i virus vengono comunemente diffusi attraverso la condivisione di file, download da Internet e allegati di posta elettronica.

I worm informatici esistono dalla fine degli anni ‘80, ma hanno preso piede solo con la diffusione delle infrastrutture di rete nelle aziende. A differenza dei virus, i worm possono propagarsi in rete senza l’intervento dell’utente.

I trojan sono progettati espressamente per sottrarre dalla rete i dati riservati. Molti tipi di trojan assumono il controllo del sistema contagiato, aprendo una “porta di servizio” da cui il criminale può accedere al sistema quando meglio crede. I trojan sono spesso utilizzati per creare botnet.

Gli spyware non sono dannosi in sé e per sé, ma sono molto fastidiosi perché spesso contagiano i browser Web, rendendoli quasi inutilizzabili. In alcuni casi, gli spyware sono mascherati da applicazioni innocue in qualche modo vantaggiose per l’utente, mentre segretamente registrano modelli di comportamento e utilizzo.

Il ransomware è un attacco che spesso cripta i file su un endpoint o un server, richiedendo poi all'utente finale di pagare un riscatto in bitcoin per ottenere la chiave di decrittografia. Quando vengono compromessi sistemi business-critical, il costo del riscatto può aumentare fino a centinaia di migliaia di dollari.

I criminali informatici utilizzano vari tipi di malware per coglierti alla sprovvista.

Contrattacco n. 2

Verifica che la rete sia protetta contro tutti i tipi di malware

Il compito dei firewall è quello di proteggere le organizzazioni da virus, worm, trojan, spyware e ransomware. Il modo migliore per tenere fede a questo obiettivo è integrare tutti i metodi di protezione con 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 comprendere tutte le seguenti funzionalità:

- **Protezione 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 dai milioni di nuove varianti di malware nel momento stesso in cui si presentano.
- **Servizio di prevenzione delle intrusioni** per impedire ai criminali di sfruttare le vulnerabilità della rete.
- **Sandbox di rete** per inviare il codice sospetto ad un ambiente isolato, basato sul cloud, dove farlo detonare e analizzare per scoprire malware finora sconosciuto.
- **Sicurezza di accesso** per applicare contromisure di sicurezza 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.

Accertarsi che ogni dispositivo collegato alla rete disponga di un software antivirus aggiornato garantisce una protezione in più contro i malware. Le organizzazioni che abbinano l'installazione di soluzioni antivirus sui PC a un firewall possono annientare molti degli strumenti di cui si servono i criminali informatici per danneggiare la rete.

Per prevenire gli attacchi, applica più livelli di protezione contro il malware.

Strategia di attacco informatico n. 3

Ricercare e danneggiare le reti più deboli

Per quanto molti fornitori di firewall si vantino di offrire sistemi di protezione eccellenti, solo in pochi hanno dimostrato l'efficacia delle proprie soluzioni. Le organizzazioni che utilizzano firewall di dubbia qualità sono erroneamente convinte che la propria rete sia protetta; al contrario, i criminali più esperti sono in grado di aggirare il servizio di prevenzione delle intrusioni utilizzando algoritmi complessi per eludere i controlli e compromettere il sistema.

Poiché alcuni firewall offrono protezione a discapito delle prestazioni, a volte le organizzazioni che li utilizzano 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 altro anello debole nel sistema di sicurezza della rete è il fattore umano. I criminali utilizzano le email di phishing per ottenere informazioni di accesso e altre autorizzazioni che gli consentano di aggirare le protezioni del firewall sferrando gli attacchi dall'interno della rete. Inoltre può accadere che i dipendenti perdano i loro dispositivi portatili o subiscano violazioni quando li utilizzano all'esterno del perimetro di sicurezza della rete.

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

Contrattacco n. 3

Scegli una piattaforma di sicurezza completa, che offra una protezione eccellente senza penalizzare le prestazioni

Scegli soluzioni di sicurezza la cui sicurezza contro il malware di rete sia testata e certificata dalla società indipendente ICSA Labs.

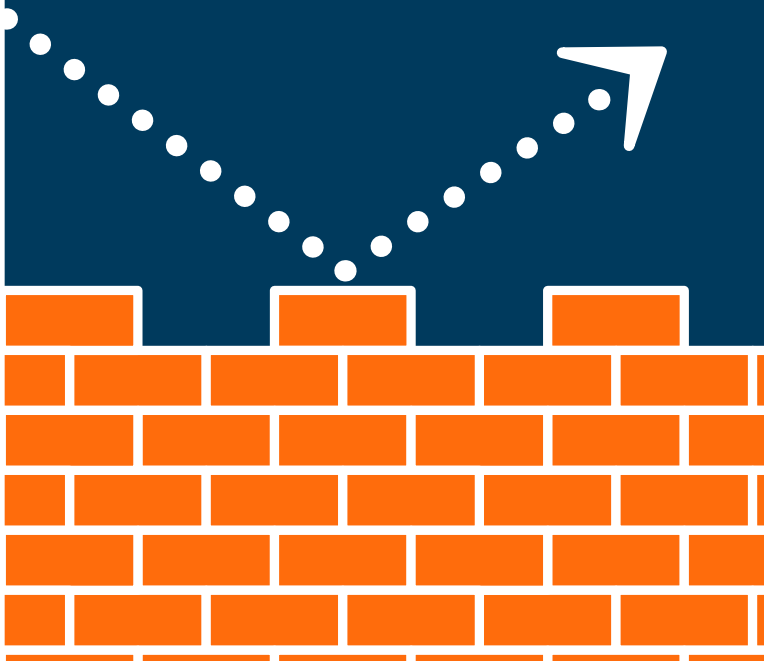
Le piattaforme multi-core consentono di eseguire la scansione di file di qualunque tipo e dimensione per gestire anche le variazioni nel flusso di traffico. Tutti i firewall necessitano di un motore che permetta di proteggere la rete dagli attacchi sia interni che esterni, ma senza compromettere le prestazioni.

Cerca un firewall dotato di una sandbox di rete che possa aiutarti a scoprire nuovi malware mirati specificamente al tuo ambiente. Ciò può fare la differenza tra una normale giornata di lavoro e una persa a causa dei file in ostaggio.

La tua strategia di sicurezza deve includere la protezione degli endpoint mobili e remoti, sia all'interno che all'esterno del perimetro.

Inoltre è necessaria una soluzione di protezione delle email per proteggerti da phishing, spam, virus, social engineering e altre minacce trasmesse per email.

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



Ogni ora compaiono nuove minacce in tutto il globo.

Strategia di attacco informatico n. 4

Trasformarsi continuamente e sferrare attacchi globali

Molti criminali informatici riescono nei loro intenti perché inventano continuamente nuovi malware e li condividono con i "colleghi" di tutto il mondo. Questo significa che in qualsiasi momento possono comparire nuove minacce a livello planetario. Molti privilegiano il metodo "saccheggio": entrano nella rete, prendono tutto ciò che capita e poi si dileguano prima che venga dato l'allarme, per andare ad attaccare un'altra rete.

Altri hanno un approccio più lento e prudente, cercando di ottenere l'accesso 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, grazie a dispositivi infettati mentre erano collegati all'esterno del perimetro di sicurezza della rete.

SONICWALL®

Contrattacco n. 4

Scegli un firewall che protegga contro gli attacchi globali

Saper reagire rapidamente è fondamentale per difendersi al meglio. Per distribuire nel firewall aziendale contromisure immediate alle minacce emergenti, scegli un fornitore di soluzioni di sicurezza che disponga di un team interno di esperti in materia altamente disponibili. L'ideale è che questo team collabori con l'intera community degli esperti in materia di protezione.

Una soluzione ad ampio spettro utilizza un catalogo di malware completo basato sul cloud, al fine di incrementare le analisi del firewall locale.

Mentre un firewall basilare si limita a identificare le minacce ed eseguire blocchi in base al criterio dell'area geografica, un firewall 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.

Per bloccare i malware globali più evoluti, investi in una protezione di portata globale.

Conclusioni

Gli attacchi informatici aumentano di continuo, ma esistono strategie di difesa efficaci. Se desideri valutare le soluzioni di protezione più adeguate per il tuo ambiente di rete, scarica il white paper Achieving Deeper Network Security.

SONICWALL®

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

Ebook-TypesOfCyberAttacks-EU-IMAG-24644

SONICWALL®