SONICWALL

COME I CYBERCRIMINALI POSSONO ELUDERE LE MISURE DI GESTIONE DELLA REPUTAZIONE

L'evoluzione dei sistemi di gestione della reputazione per la sicurezza delle e-mail

Abstract

Con l'evoluzione della tecnologia, i criminali informatici sviluppano costantemente nuove tattiche per mettere a segno nuovi attacchi. La lista RBL (Real-time Blackhole List) è stata sviluppata nel 1997 e costituisce il fondamento dell'odierno formato DNSBL (DNS-based Blackhole List). Tuttavia i criminali informatici compiono attacchi in grado di minare e aggirare i sistemi di gestione della reputazione IP. È quindi importante che i professionisti della sicurezza si aggiornino e siano sempre un passo avanti per prevenire questi attacchi.

Come i cybercriminali eludono i sistemi di gestione della reputazione IP

Con la crescente diffusione dei sistemi di verifica della reputazione degli indirizzi IP, gli hacker hanno iniziato a concentrare i propri sforzi per eludere questi sistemi. Gli autori delle minacce utilizzano sempre più spesso e-mail di phishing e spam per camuffarsi da fonte affidabile e utilizzare i sistemi di posta elettronica aziendale e i dipendenti per infliggere danni alle aziende. I "phisher" si mascherano da partner o amico fidato e inviano e-mail che puntano a compromettere server di posta legittimi in aziende che godono di una buona reputazione, oppure a violare gli account di web-mail di ISP o ASP come Yahoo® o Gmail®. In questo modo, inviando messaggi dannosi insieme a messaggi innocui dai server compromessi di aziende attendibili, i criminali informatici riescono a evitare o a posticipare l'inserimento nelle liste dei tradizionali sistemi di gestione della reputazione IP.

Pur manipolando i propri indirizzi IP, i criminali informatici non alterano tutti gli aspetti di un messaggio spam o di phishing in modo uniforme. Come altre organizzazioni a scopo di lucro, anche i cybercriminali tagliano i costi generali riducendo la complessità

Per prepararsi alle future minacce diffuse attraverso l'e-mail bisogna imparare dal passato.

e tendono perciò a riutilizzare gli indirizzi IP, i contenuti, i layout, i collegamenti ipertestuali e pure le immagini. Ciò rappresenta un buona opportunità per realizzare un ulteriore livello di difesa tramite l'identificazione e la gestione della reputazione che vada oltre i soli indirizzi IP.

Uno sguardo al passato: l'evoluzione della gestione della reputazione

Il primo sistema di gestione della reputazione è iniziato con la lista RBL (Real-time Blackhole List). La primissima lista RBL è stata sviluppata nel 1997 da Paul Vixie per il sistema di prevenzione degli abusi via posta elettronica MAPS (Mail Abuse Prevention System). Mediante l'invio dei messaggi a un link di rete che bloccava il traffico in arrivo anziché inoltrarlo, nelle intenzioni di Vixie il "buco nero" doveva servire a bloccare il traffico e-mail proveniente da siti che inviavano direttamente o consentivano i messaggi spam. La lista RBL originaria consisteva in un elenco di siti sospetti che veniva inviato tramite il protocollo BGP (Border Gateway Protocol) agli amministratori di sistema che si abbonavano al servizio, i quali potevano poi utilizzare l'elenco per bloccare il traffico TCP/IP in arrivo da quei siti.

La gestione delle reputazioni con RBL ha rappresentato indubbiamente un significativo passo avanti, ma non era priva di problemi. Il sistema MAPS verificava meticolosamente l'accuratezza dei siti prima di pubblicarli nella lista RBL. Se questa perizia contribuiva da un lato a ridurre i falsi positivi, dall'altro comportava notevoli ritardi nella capacità di reagire prontamente agli attacchi. Nel tempo, MAPS ha sviluppato dei client RBL che si integravano con i software di posta elettronica per consentire agli amministratori di personalizzare la propria lista RBL, in modo da rifiutare le e-mail in arrivo in base alle impostazioni del server.

La lista RBL del sistema MAPS ha gettato le basi per lo sviluppo del formato DNSBL. Il servizio Internet DNS (Domain Name System) converte i nomi di dominio/host in indirizzi IP (risoluzione DNS) e gli indirizzi IP nel corrispondente nome di dominio/host (risoluzione inversa) con l'ausilio di un server DNS. La DNSBL non è rimasta una semplice lista discreta, ma ha aggiunto diversi standard per l'inserimento e la rimozione dinamici degli indirizzi IP dalla lista Blackhole. I fornitori di servizi DNSBL potevano così distribuire liste aggiornate tramite il servizio IDNS (Internet Domain Name Service) utilizzando un formato standardizzato. I primi sviluppatori di liste DNSBL hanno aggiunto criteri per rilevare ad esempio se un server di posta mittente usa opzioni di relay o proxy aperti potenzialmente sfruttabili o se un server di posta invia spam a un sistema "honeypot", progettato per attirare e raccogliere spam a scopo d'identificazione e analisi.

Oggi esistono decine di servizi DNSBL e la maggior parte dei server di posta è in grado di interrogarli per verificare la reputazione degli indirizzi IP. Tuttavia ogni servizio adotta criteri differenti per aggiungere, rimuovere o conservare gli indirizzi IP nelle proprie liste, per cui alcuni elenchi potrebbero non contenere indirizzi IP potenzialmente pericolosi o potrebbero includere per errore alcuni indirizzi validi.

Conclusioni

La posta elettronica è un vettore primario di minacce, che i criminali informatici utilizzano costantemente per mettere a segno i propri attacchi. Le e-mail di phishing rappresentano il punto di partenza di molti degli attacchi più efficaci perpetrati alle reti aziendali. Con l'aumento dei fenomeni di spear phishing e di whaling, è sempre più difficile distinguere le e-mail dannose dalle comunicazioni aziendali legittime. Per tale motivo è indispensabile assicurarsi che il proprio sistema di gestione della reputazione offra una protezione efficace contro le nuove minacce diffuse attraverso la posta elettronica.

Per saperne di più: leggi il nostro documento "Gestione avanzata della reputazione per contrastare le minacce e-mail".

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