Cisco Email Security: Informazioni sul motore di scansione adattiva del contesto (CASE)

Sommario

Introduzione

L'aumento del volume di minacce miste è stato drammatico. Molte delle più significative epidemie di virus degli ultimi due anni sono state associate alla consegna di spam - il che significa che il payload del virus crea un esercito di computer "zombie" - che vengono utilizzati per inviare spam, phishing, spyware e ancora più virus. Gli spyware trasmessi tramite e-mail raddoppiano ogni sei mesi e non è insolito che gli URL spammati installino "keylogger" che rubano nomi utente e password. I virus possono anche essere usati per creare una rete di zombie per lanciare un attacco distribuito di massa contro i servizi negati, come quando la variante Mydoom.B ha messo offline il sito della SCO con un attacco coordinato.

Cosa spinge l'improvviso aumento di minacce miste? In breve, sono i soldi. Con la diffusione delle tecniche anti-spam di prima generazione (come le liste nere e i filtri dei contenuti), i metodi tradizionali (come l'invio di spam da un gruppo fisso di server contenenti un'"offerta" nel testo del messaggio) sono diventati meno redditizi. Con un numero maggiore di reti che utilizzano la tecnologia antispam, un numero minore di messaggi "semplici" trasmettono il messaggio oltre i filtri antispam e nella casella di posta del destinatario. Ciò danneggia i margini di profitto degli spammer e li ha costretti ad adattarsi a questi cambiamenti.

Gli spammer hanno gestito la situazione in due modi distinti:

1. Stanno inviando ancora più spam con la speranza che quello che perdono in termini di velocità di consegna, compenseranno in volume.
2. Si stanno rivolgendo ad attacchi misti per mascherare i loro messaggi e aumentare i loro profitti per messaggio.

La seconda tecnica spesso diventa un'attività criminale. Sono state create reti di criminalità organizzata per eseguire attacchi e trarre profitto da virus, phishing e altre minacce. Nel 2004, un individuo di nome John Dover è stato arrestato dopo aver scambiato più di due milioni di numeri di carte di credito, che sono stati rubati attraverso attacchi di phishing.

Anche le tecniche utilizzate negli attacchi misti sono diventate sempre più sofisticate. Il virus Sober.N impiegava e-mail, download web, trojan e zombie. I filtri tradizionali per l'analisi dei

contenuti non sono adatti a queste minacce intelligenti. Molti utenti dei filtri antispam di prima generazione hanno scoperto di dover dedicare sempre più ore alla "formazione" dei filtri o alla scrittura di nuove regole. Tuttavia, nonostante questi sforzi, il loro tasso di cattura e il loro throughput sono entrambi in calo. Ne consegue che i costi aumentano in quanto più sistemi sono necessari per tenere il passo con il carico, mentre più tempo di amministrazione viene utilizzato per gestire ogni sistema.

Cisco Email Security ha risolto queste minacce con un'esclusiva tecnologia di difesa dalle minacce miste nota come Context Adaptive Scanning Engine (CASE). La tecnologia CASE di Cisco Email Security viene utilizzata per fermare sia lo spam tradizionale che i sofisticati attacchi basati su zombie. Questa stessa tecnologia di scansione viene utilizzata anche per prevenire virus e malware fino a 42 ore prima della disponibilità della firma, con una singola scansione unificata per l'efficienza.

Case, rilevamento di minacce di blend nel contesto

I filtri di prima generazione sono stati progettati per esaminare il contenuto di un messaggio e prendere una decisione. Ad esempio, se la parola "free" appare in un messaggio più di due volte, insieme alla parola "herbal", probabilmente è spam. Questo approccio è relativamente facile da sconfiggere per gli spammer usando caratteri o numeri nascosti al posto delle lettere, come "f0r y0u" al posto di "per te". Le tecniche di seconda generazione, come i filtri bayesiani, hanno tentato di superare questa limitazione imparando a distinguere automaticamente le caratteristiche della posta indesiderata e della posta elettronica legittima. Ma queste tecniche si sono rivelate troppo difficili da allenare, troppo tardi per reagire, e troppo lente per scannerizzare.

Date le tecniche avanzate di offuscamento utilizzate con lo spam odierno, i filtri allo stato dell'arte devono esaminare la posta in arrivo nel contesto completo. CASE utilizza tecniche avanzate di apprendimento automatico che emulano la logica utilizzata da un essere umano che valuta la legittimità di un messaggio. Un lettore umano, così come la tecnologia CASE di Cisco Email Security, fa quattro domande fondamentali:

1. Chi mi ha mandato il messaggio?
2. Dove mi portano i link nel messaggio?
3. Come è stato costruito il messaggio?
4. Contenuto del messaggio

Seguire un esame di ogni area logica valutata.

Chi?

Come accennato in precedenza, i filtri antispam di prima generazione si basano principalmente sulle ricerche per parole chiave per identificare lo spam. Nel 2003, Cisco (IronPort) ha rivoluzionato il settore della sicurezza e-mail introducendo il concetto di filtro della reputazione. Mentre il filtro dei contenuti poneva la domanda "Che cosa c'è nel messaggio?", il filtro della reputazione poneva la domanda "Chi ha inviato il messaggio?". Questo semplice ma potente concetto ha ampliato il contesto in cui vengono valutate le minacce. Nel 2005, quasi tutti i principali fornitori di prodotti per la sicurezza commerciale avevano adottato un sistema di reputazione.

Per determinare la reputazione è necessario esaminare un'ampia serie di dati sul comportamento di un determinato mittente (per mittente si intende un indirizzo IP che invia posta). Cisco prende in considerazione oltre 120 parametri diversi, tra cui il volume delle e-mail nel tempo, il numero di

"trappole per lo spam" riscontrate dall'IP, il paese di origine, se l'host è compromesso e molti altri. Cisco dispone di un team di statistici che sviluppa e gestisce algoritmi che elaborano i dati per generare un punteggio di reputazione. Questo punteggio viene quindi reso disponibile per l'appliance Cisco Email Security (ESA) ricevente, che può quindi limitare il mittente in base all'affidabilità. In breve: più uno spammy appare al mittente, più lentamente diventa. Il filtro della reputazione consente inoltre di risolvere i problemi associati all'aumento dei volumi di posta elettronica tramite il rifiuto o la limitazione delle connessioni prima dell'accettazione del messaggio, migliorando notevolmente le prestazioni e la disponibilità del sistema di posta. I filtri di reputazione Cisco ESA bloccano più dell'80% della posta indesiderata in arrivo, circa il doppio della velocità di ricezione dei sistemi della concorrenza.

Dove?

Mentre la combinazione di analisi dei contenuti e-mail e reputazione era all'avanguardia nel 2003, la sofisticata tattica di spammer e autori di virus continua a crescere. In risposta, Cisco (IronPort) ha introdotto la nozione di reputazione Web, un nuovo vettore fondamentale per ampliare il contesto in cui un messaggio viene valutato. Analogamente all'approccio utilizzato per calcolare la reputazione di un'e-mail, Cisco Web Reputation prende in considerazione più di 45 parametri relativi al server per valutare la reputazione di un determinato URL. I parametri includono il volume di richieste HTTP indirizzate all'URL nel tempo, se l'URL è ospitato su un indirizzo IP con un punteggio di reputazione basso, se l'URL è associato a un host PC noto come "zombie" o infetto e la data del dominio utilizzato dall'URL. Come per la reputazione dell'e-mail, questa reputazione Web viene misurata utilizzando un punteggio granulare, che consente al sistema di affrontare le ambiguità di minacce sofisticate.

Come?

Un altro approccio innovativo all'analisi contestuale di Cisco Email Security è esaminare la costruzione di un messaggio. I client di posta legittimi, ad esempio Microsoft Outlook, creano i messaggi in modo univoco utilizzando la codifica MIME, HTML o altri metodi simili. L'esame della costruzione di un messaggio può rivelare molto sulla sua legittimità. Un esempio significativo di ciò si verifica quando un server di spam tenta di emulare la costruzione di un client di posta legittima. Questo è difficile da fare, e un'emulazione imperfetta è un indicatore affidabile di un messaggio illegittimo.

Cosa?

Un'analisi contestuale completa deve prendere in considerazione il contenuto di un messaggio, ma, come detto in precedenza, l'analisi del contenuto da sola non è un approccio sufficiente per identificare la posta illegittima. La tecnologia CASE di Cisco Email Security esegue un'analisi completa dei contenuti utilizzando tecniche di apprendimento automatico allo stato dell'arte. Queste tecniche esaminano il contenuto del messaggio e lo classificano in varie categorie: è finanziario, pornografico o contiene contenuto che è noto per essere correlato ad altri spam? Questa analisi del contenuto viene inserita nel CASE insieme agli altri attributi (Who, Where, How e What) per valutare il contesto completo del messaggio.

CASO in azione

A causa della vasta gamma di dati analizzati da CASE, la tecnologia è utilizzata in una vasta gamma di applicazioni di sicurezza, tra cui IronPort Anti-Spam (IPAS), Graymail e Virus Outbreak

Filters (VOF). Nell'esempio seguente viene illustrato come utilizzare CASE per bloccare la posta indesiderata. Il contenuto del messaggio è quasi identico a quello dell'organizzazione che riceve il phishing, quindi l'analisi del contenuto del messaggio non identificherebbe alcuna minaccia. Per i filtri basati sul contenuto, questo messaggio sembra essere una comunicazione legittima. Per stabilire se il messaggio è indesiderato, i filtri che si basano principalmente sul messaggio "Cosa" potrebbero essere facilmente ingannati per riconoscere la legittimità del messaggio. Tuttavia, un'analisi del contesto completo del messaggio delinea un quadro diverso.

- L'indirizzo IP del server di posta elettronica di invio è sospetto: ha avuto un aumento improvviso di volume e il dominio, in cambio, non accetta la posta.
- L'URL dell'e-mail punta a un server che sembra essere in una rete a banda larga consumer.
- L'URL annunciato nel messaggio è diverso dall'URL "effettivo" a cui l'utente accede facendo clic sul link.

Se tutti e tre questi fattori vengono considerati nel contesto, diventa chiaro che questo non è un messaggio legittimo, ma in realtà è un attacco di spam.

"Filtri dei contenuti" tradizionali
Ricerca dei filtri dei contenuti

Cosa? Contenuto del messaggio legittimo.

Verdetto: SCONOSCIUTO

Scansione adattiva del contesto
Risultati di CASE

Cosa? Contenuto del messaggio legittimo.
Come? Costruzione messaggi emula Microsoft C
di Outlook.
Chi?
1) Aumento improvviso del volume di e-mail invia
2) In cambio, il server di posta non accetta la pos
3) Server di posta situato in Ucraina.

Dove?
1) Mancata corrispondenza tra il dominio del sito
di visualizzazione e dell'URL di destinazione regis
il giorno fa.
2) Sito Web ospitato su una rete a banda larga di
consumo.
3) I dati "Whois" mostrano il proprietario del domi
come spammer conosciuto.

Verdetto: Block (Blocca)

Quando si utilizza CASE nei filtri epidemie di virus, vengono applicate le stesse funzionalità di punteggio e apprendimento automatico, anche se a un set di dati regolato separatamente. I filtri epidemie di virus sono una soluzione antivirus preventiva offerta da Cisco e basata sulla tecnologia CASE. La soluzione Outbreak Filters analizza i messaggi sia in base alle norme epidemie in "tempo reale" (rilasciate da Cisco Talos per specifici focolai) che alle regole adattive "always on" (che risiedono su CASE in ogni momento), proteggendo gli utenti contro i focolai prima che abbiano avuto la possibilità di formarsi completamente. CASE consente ai filtri epidemie di virus di rilevare e proteggere in diversi modi con precisione le epidemie di virus. In primo luogo, CASE è in grado di analizzare rapidamente i messaggi in base a parametri quali l'estensione del file dell'allegato, le dimensioni del file, il nome del file, le parole chiave del nome del file, l'estensione effettiva del file e gli URL incorporati. Poiché la tecnologia CASE analizza i messaggi a questo livello di dettaglio, Cisco Talos può emettere regole sulle epidemie estremamente granulari, che assicurano una protezione accurata contro un'epidemia con un numero minimo di

falsi positivi. CASE può ricevere in modo dinamico le regole aggiornate sui focolai, che assicurano la protezione contro i focolai più recenti.

Oltre all'analisi dei messaggi basata sulle regole epidemie, la tecnologia CASE analizza i messaggi basati sulle regole adattive. Adaptive Rules sono euristiche e algoritmi finemente ottimizzati che esaminano i messaggi in arrivo per individuare eventuali malformazioni e caratteristiche di spoofing che indicano la presenza di virus. Oltre a questi parametri, le regole adattive assegnano un punteggio ai messaggi in base al punteggio del virus (SBVS) SenderBase. Il punteggio SBVS è simile al punteggio SBRS (SenderBase Reputation Score), ma con una classificazione basata sulla probabilità che la parte mittente invii e-mail virali, anziché spam. La maggior parte dei messaggi e-mail virali viene inviata da macchine "zombie" precedentemente infette, quindi l'identificazione e il punteggio di questi invianti è un fattore essenziale nella cattura dei virus.

La tecnologia CASE di Cisco Email Security consente ai filtri epidemie di virus di arrestare le epidemie molto prima delle soluzioni antivirus tradizionali, perché il CASE esamina i messaggi in diversi modi. È in grado di analizzare numerose caratteristiche degli allegati, del contenuto e della costruzione dei messaggi, nonché di analizzare i messaggi in base alla reputazione del mittente. Inoltre, poiché CASE funziona anche come motore IronPort Anti-Spam e Reputation Filters, un messaggio deve essere analizzato una sola volta per tutte queste applicazioni.

Prestazioni elevate, costi ridotti

La logica alla base della tecnologia CASE può essere molto sofisticata e quindi molto impegnativa da elaborare. Per massimizzare l'efficienza, CASE utilizza un'esclusiva tecnologia di "uscita anticipata". L'uscita anticipata dà la priorità all'efficacia della miriade di regole elaborate da CASE. La tecnologia CASE applica per prime le regole con il massimo impatto e il minor costo. Se si raggiunge un verdetto statistico (positivo o negativo), non vengono eseguite regole aggiuntive, risparmiando risorse di sistema. L'eleganza in questo approccio è avere una buona comprensione dell'efficacia di ogni regola. CASE controlla e adatta automaticamente l'ordine di esecuzione delle regole in base alle modifiche dell'efficacia.

Il risultato di un'uscita anticipata è che la tecnologia CASE elabora i messaggi a una velocità superiore del 100% rispetto a un filtro tradizionale basato su regole. Ciò presenta vantaggi significativi per i grandi ISP e le aziende. Ma ha anche dei benefici per le piccole e medie imprese. L'efficienza di CASE, unita all'efficacia del sistema operativo AsyncOS di Cisco Email Security, consente di implementare ESA con tecnologia AsyncOS e CASE su hardware a costo molto contenuto, riducendo i costi di capitale.

Un altro modo in cui la tecnologia CASE si traduce in costi ridotti consiste nell'eliminare il sovraccarico amministrativo. La richiesta CASE viene ottimizzata e aggiornata automaticamente migliaia di volte al giorno. Cisco Talos mette a disposizione ingegneri qualificati, tecnici multilingue e personale statistico. Gli analisti Cisco Talos dispongono di strumenti speciali che evidenziano le anomalie nel flusso di posta rilevate nella rete di un cliente Cisco Email Security o nei modelli di traffico di posta globale. Cisco Talos genera nuove regole che vengono automaticamente applicate al sistema in tempo reale. Cisco Talos gestisce anche un enorme corpus di "spam and ham", utilizzato per addestrare varie regole usate da CASE. Le regole CASE aggiornate automaticamente non richiedono agli amministratori di regolare e modificare il filtro o di passare del tempo attraverso le quarantene di posta indesiderata.

Riepilogo

Spam, virus, malware, spyware, attacchi di negazione del servizio e attacchi di raccolta di directory sono tutti guidati dallo stesso motivo di fondo - profitti. Tali profitti sono conseguiti attraverso la vendita o la pubblicità di merci o il furto di informazioni. I profitti derivanti da queste vendite sono alla base di attacchi sempre più sofisticati, sviluppati da tecnici professionisti. I sistemi avanzati di sicurezza e-mail devono analizzare un messaggio nel contesto più ampio possibile per contrastare queste minacce. La tecnologia Context Adaptive Scanning Engine di Cisco Email Security pone le quattro domande fondamentali: Chi, dove, cosa e come eliminare messaggi legittimi da minacce miste.

- "Chi" è la reputazione del mittente nell'e-mail - chi ha inviato il messaggio.
- "Dove" è la reputazione della fonte che ospita il sito - analizzando dove il link potrebbe portarvi.
- "What" è un'analisi del contenuto del messaggio - quello che il messaggio contiene (i sistemi di prima generazione si affidano spesso solo al tipo di analisi "What").
- Infine, "Come" è un'analisi di come il messaggio è costruito.

Questa struttura di base per l'analisi di Who, Where, What e How (Chi, dove, cosa e come) è ideale per l'arresto della posta indesiderata, così come per la prevenzione di epidemie di virus, attacchi di phishing, spyware via e-mail o altre minacce e-mail. I set di dati e le regole di analisi vengono ottimizzati specificamente per ogni minaccia. La tecnologia CASE consente a Cisco ESA di arrestare la più ampia gamma di minacce con la massima efficienza possibile elaborando queste minacce su un unico motore ad alte prestazioni.