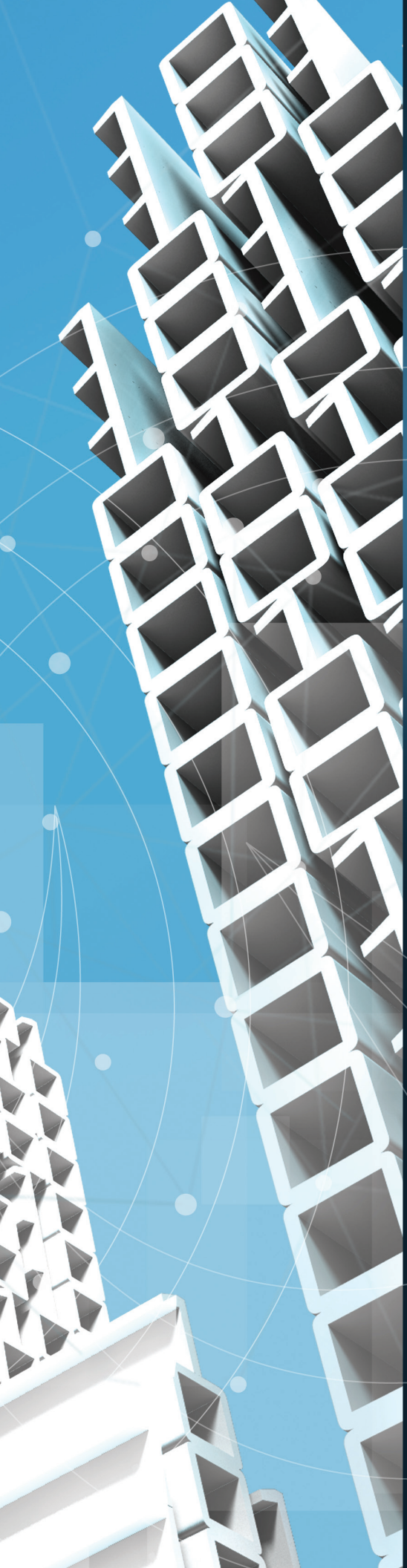

Websense® in breve

di Patrick Murray, Senior Director of Product Management

ATTACCHI AVANZATI E MIRATI:

DALLA PAURA, L'INCERTEZZA E I DUBBI AI FATTI

Websense ti permette di essere sempre un passo avanti rispetto alle minacce. Grazie ai nostri strumenti di Web filtering, da oltre 15 anni, analizziamo e classifichiamo contenuti e offriamo la massima sicurezza di Web, e-mail e Dati (DLP) difendendo anche quelle aree che non verrebbero protette dai sistemi di sicurezza tradizionali.

websense®
ESSENTIAL INFORMATION PROTECTION™

"APT" (Advanced Persistent Threat – Minacce Avanzate e Persistenti) è il termine più discusso di quest'anno. Ma che cosa significa esattamente? Una strategia di marketing martellante e la diffusione di paura, incertezza e dubbi hanno contribuito ad offuscare i i reali pericoli derivanti da queste minacce avanzate, ma soprattutto mirate, che minacciano le organizzazioni di tutte le dimensioni. Questa presentazione si ripropone di:

1. spiegare come la maggior parte dei criminali informatici utilizza attachi avanzati di tipo mirato (APT) per violare la sicurezza dei dati
2. esplorare l'anatomia di un attacco mirato
3. offrire soluzioni per una difesa efficace

Perché preoccuparsi delle APT?

Le organizzazioni di grandi dimensioni con un'enorme ricchezza di proprietà intellettuali (come i codici sorgente) sanno perfettamente di essere un target molto ambito dai cybercriminali. Ma le organizzazioni di più piccole dimensioni non sono preoccupate. "La mia società in Ohio genera un fatturato di 10 milioni di dollari all'anno. Non credo proprio che i criminali informatici coreani o cinesi vengano a bussare alla mia porta nei prossimi giorni." È vero che non verranno. Ma è altrettanto probabile che altri perpetratori di attacchi informatici lo faranno.

Per molte aziende, le APT non sono una grande preoccupazione in quanto, per definizione, sono essenzialmente utilizzate da alcuni governi con l'intento di causare problemi ad altri governi o ad aziende di grandi dimensioni. Ma le APT sono anche un prototipo per altri attacchi mirati che vittimizzano altre aziende, di tutte le forme e dimensioni. È un dato di fatto: la tecnologia delle APT usata dalla Cina per attaccare Google è ora usata da numerosi criminali informatici per rubare dati da organizzazioni come la tua.

I Websense® Security Labs™ hanno dato il via ad un'analisi approfondita delle APT in circolazione e ha diagrammato l'emergere di questi exploit. Per saperne di più sui Security Labs...

In che modo le APT sono riuscite ad entrate nel libero mercato

Prova a immaginare un paese che indossi un giubbotto antiproiettile. Per trapassare il giubbotto, alcuni governi o agenti da essi sponsorizzati investono un enorme capitale per inventare speciali munizioni che riescano eventualmente a trapassare quest'armatura. In breve tempo, queste speciali munizioni diventano disponibili sul mercato informatico e i criminali le usano in tutti i tipi di crimini cibernetici. Lo stesso ciclo è applicabile alla tecnologia del malware.

Esaminiamo ora una classica APT e come le tecniche usate siano passate rapidamente nelle mani dei malintenzionati dell'informatica.

Il ciclo di vita delle tecnologie del malware

Gli attacchi Aurora del 2009 sono stati tra le prime APT ad essere ambiamente pubblicizzate. Aziende quali Google, Adobe e Rackspace furono infatti prese di mira dalle APT sponsorizzate da un governo, nei mesi di novembre e dicembre del 2008. Il 12 gennaio 2009, Google annunciò di essere stata attaccata. Dopo due giorni, i codici che sfruttano vulnerabilità, noti come "zero-day exploit", furono rivelati al pubblico. Dopo nove giorni, Microsoft applicò una patch a difesa della sua vulnerabilità principale. In questo periodo,

soltanto il 26% dei produttori di programmi antivirus furono in grado di identificare l'exploit in quanto era completamente nuovo. D'altro canto, nel giro di un solo mese, Websense® ThreatSeeker® Network rilevò più di 200 nuovi siti web che usavano lo stesso tipo di exploit per la diffusione di malware. Le APT si propagarono con la rapidità di un incendio alimentato dalle organizzazioni criminali che disponevano di nuove munizioni da usare contro i propri target più ambiti, ossia aziende con informazioni sulla clientela o con numeri di carte di credito che potevano essere rapidamente convertiti in soldi contanti.

Anatomia di un attacco mirato

Come funzionano esattamente le APT e gli attacchi mirati? Esaminiamo ora un caso concreto di APT.

Advanced: Gli autori di attacchi informatici usano una serie di tecnologie complicate di raccolta di dati importanti. L'azione inizia normalmente mesi prima dell'attacco vero e proprio, ossia del furto di dati importanti da un'organizzazione.

Ad esempio:

- *Gli autori di attacchi informatici si infiltrano e si impossessano del server di un'altra azienda (non dell'azienda presa di mira). Questo viene spesso effettuato con l'inserimento di un codice maligno, tramite una query SQL, in una vecchia tabella su una pagina web ignorata da tempo o in un'applicazione web non protetta. Queste verranno usate in seguito come il punto anonimo "dead drop" e la pista che si seguirà per arrivare alla sorgente, finirà qui.*
- *Un elemento di malware personalizzato viene inviato all'account e-mail personale di un dipendente (presupponendo che i dipendenti controllino la loro e-mail personale tutti i giorni dal lavoro). Questo malware inizia a viaggiare lungo la rete creando una mappa e verificando le misure di sicurezza implementate. Nota: la sorveglianza dell'individuo target inizia prima della sorveglianza della rete. Molto spesso il target di questa e-mail può venire identificato tramite una ricerca condotta nei profili definiti in un social web o in LinkedIn o in Facebook,o tramite semplici query di ricerca, ad esempio, di dirigenti nell'ambito di siti Web aziendali, ecc. In una società esiste un'enorme quantità di informazioni disponibili su ogni possibile target, che facilita al massimo l'invio da parte di programmatori sociali di un'invitante e-mail a un soggetto nella sua lingua nativa, usando le sue preferenze e determinate informazioni che possono servire a incoraggiarlo ad aprire l'e-mail inviata. Gli autori di attacchi informatici possono già essere diventati "amici" di questo soggetto, nell'ambito dei siti social, ed aver raccolto le necessarie informazioni.*

Persistent: Gli autori di attacchi informatici sono determinati a conseguire il loro obiettivo. Condurranno attività di monitoraggio con la massima pazienza, perseveranza e tenacia al fine di identificare le aree più vulnerabili. Ripeteranno più volte i loro tentativi e cambieranno tattica, qualora vengano identificati.

- *Nel nostro esempio, il malware ha ora mappato la rete e ha inviato informazioni agli autori di attacchi informatici sui protocolli di sicurezza implementati compreso gli indirizzi dei programmi AV e dei firewall proxy. A questo punto gli autori di attacchi informatici sanno come infiltrarsi e, ancora più importante, sanno dove si trova con molta probabilità la ricompensa del loro lavoro.*

Threat: Gli autori di attacchi informatici tendono ad usare molteplici vettori di attacco compreso malware specificatamente sviluppato e vulnerabilità "zero-day" non ancora note.

- *Nel nostro esempio, abbiamo già visto un tipo di malware personalizzato utilizzato per condurre operazioni di sorveglianza. Siamo ora giunti al codice killer.*

- *Viene inviata una nuova e-mail all'account personale di un altro dipendente che ha accesso a dati importanti. L'e-mail trasporta un payload di malware tecnologicamente raffinato che identifica i sistemi da evitare e rileva i punti di residenza dei dati e sa come sottrarli senza essere immediatamente intercettato. Il codice è anche polimorfico in quanto si aggiorna automaticamente da sé per continuare a impedire la sua intercettazione da parte dei programmi AV e delle altre misure di sicurezza. (Occorre tenere presente che questo non è una semplice "botnet" che conduce una ricerca online sulle credenziali bancarie al fine di svuotare il relativo conto corrente. Questi autori di attacchi hanno ambizioni molto più serie. Vogliono le proprietà intellettuali, i segreti industriali e altri dati sensibili che possono usare per imbarazzare o per sfruttare l'individuo o l'azienda che hanno preso di mira).*
- *I dati vengono spesso sottratti molto lentamente senza che IT o il gruppo preposto alla sicurezza dei dati se ne renda conto. Soltanto dopo un incidente di tipo diverso, i gruppi preposti alla sicurezza dei dati diverranno sospettosi riguardo a movimenti illeciti nei log e questa è di solito la prima volta che il collegamento a indirizzi IP sospetti (ricordi il punto 1?) viene notato.*

In che modo Websense ti aiuta a difenderti dalle APT e dagli attacchi mirati?

Questi attacchi utilizzano tecniche sofisticate e miste che traggono vantaggio sia dai canali web sia da quelli e-mail per diffondere malware e utilizzano gli stessi canali per l'estrusione di dati confidenziali. Spesso il malware è completamente sconosciuto e viene appositamente sviluppato per eludere le difese tradizionali.

Websense® TRITON™ è la nostra soluzione unifica per la sicurezza di Web, e-mail e dati studiata specificatamente per ogni tipo di attacco misto. I sistemi di analisi di sicurezza integrata di Websense® Advanced Classification Engine (ACE) – il cuore della soluzione TRITON – monitorano tutti i contenuti in entrata e in uscita da un'organizzazione. TRITON analizza in tempo reale sia il contesto che il contenuto (compreso qualsiasi tipo di codice) di tutte le pagine Web e di tutte le e-mail.

Analizza inoltre i contenuti inviati all'esterno per accertare che i dati confidenziali non vengano inviati in modo inappropriato. Al contrario dei sistemi di difesa con un raggio d'azione limitato, quali antivirus, filtri URL, firewall e sistemi basati sulla reputazione, la sicurezza integrata di TRITON identifica e protegge contro qualsiasi minaccia, sia che si tratti di una minaccia nota o meno.

In che modo la soluzione Websense® TRITON ™ gestisce gli attacchi mirati e di tipo misto più efficacemente di qualsiasi altra tecnologia di sicurezza?

Websense TRITON è l'unica soluzione di sicurezza realmente unificata funzioni con tutte queste importanti caratteristiche:

1. **Consapevolezza di una sicurezza condivisa:** I sistemi di analisi di sicurezza integrata di Websense® Advanced Classification Engine (ACE) abbinano servizi di identificazione di malware e di protezione (compreso programmi antivirus e filtri URL) con un'avanzata ispezione dei codici e con sistemi di analisi comportamentale, euristica, di exploit, reputazione e altri tipi di scansione per identificare minacce sia note sia non (dai virus standard più diffusi a un Bot acquistato o ad un Trojan o ad uno script avanzato e appositamente programmato per attaccare le vulnerabilità di un'applicazione o di un browser). ACE

integra i risultati ottenuti dai singoli componenti della scansione (ad es. servizi di reputazione + antivirus +analisi di exploit, ecc) e prende una decisione integrata e intelligente mirata al traffico da consentire o da bloccare. La potenza di ACE consente TRITON di integrare l' "intelligence" delle nostre tecnologie di sicurezza applicate a web, e-mail e dati, nella prevenzione di intrusioni provenienti da attacchi informatici mirati che non vengono normalmente rilevati dalle tecnologie di sicurezza più tradizionali.

2. **Ispezione dei contenuti in uscita:** La maggior parte delle tecnologie di sicurezza tradizionali ispezionano soltanto le minacce in entrata e ignorano le comunicazioni in uscita. Le APT, tuttavia, così come altri attacchi mirati, sono più sofisticati degli attacchi tradizionali e sfondano molto più facilmente le difese programmate. Se e nel momento in cui questi attacchi si infiltrano nella rete, è essenziale ispezionare e proteggere la trasmissione di dati in uscita per bloccare con successo gli attacchi di sottrazione di dati confidenziali.

   Questo è il motivo per cui Websense offre una funzione di scansione dei contenuti in uscita in modo da essere certi che un computer infetto non possa comunicare all'esterno dati confidenziali. Websense applica una tecnologia di prevenzione dalla perdita di dati (DLP) di livello "enterprise" mediante l'identificazione e il monitoraggio di dati confidenziali trasmessi tramite il web, le e-mail ed altri canali al fine di assicurare che raggiungano soltanto destinazioni autorizzate e che non cadano nelle mani di autori di attacchi informatici.

   La soluzione Websense TRITON analizza anche le comunicazioni crittografate che vengono spesso utilizzate negli attacchi misti per mascherare la trasmissione di dati confidenziali in uscita, e blocca le trasmissioni SSL che non rispondono a standard comuni. Websense® TRITON Web Security Gateway sottopone a scansione tutte le comunicazioni in uscita indicative di centri di comando e di controllo dei botnet che potrebbero tentare una comunicazione di tipo "phone home".

3. **Copertura completa, flessibilità e facilità d'uso:** Per quanto un sistema di sicurezza offra funzioni di scansione al fine della rilevazione di malware, di euristica per il malware non ancora noto e di controllo delle comunicazioni via back-channel per prevenire la perdita di dati, potrebbe sempre esistere qualche area non protetta. A meno che la copertura non si estenda ai dispositivi mobili e alle filiali, questi "anelli deboli" della catena potrebbero pregiudicare la tenuta del sistema di sicurezza adottato. A meno che la soluzione non disponga di flessibilità d'implementazione (con soluzioni in sede, tramite host e/o miste) non potrà garantire una futura crescita o un rapido adattamento alle mutevoli esigenze di un'organizzazione. E a meno che non sia facile da gestire, con la granularità e la semplicità di una console di gestione unificata, potrebbe non essere efficace.

   La sicurezza di Websense TRITON rappresenta l'unica soluzione effettivamente unificata in grado di soddisfare tutti i criteri sopra descritti.

Conclusione: le nuove minacce richiedono nuove soluzioni di sicurezza

Se è vero che le APT non prendono di mira tutti, è altrettanto vero che occorre essere consapevoli di come funzionano in quanto rappresentano le tecniche usate dai criminali informaci nei loro attacchi mirati al furto di dati confidenziali da tutti i tipi di organizzazione.

La difesa contro questi attacchi mirati richiede un nuovo approccio. Scopri come puoi proteggere i tuoi dati, iniziando oggi stesso, con le soluzioni di sicurezza Websense®.