SONICWALL™

IL LATO OSCURO DELLA CRITTOGRAFIA

Perché è necessario decrittografare il traffico per bloccare le minacce nascoste

Abstract

Probabilmente la maggior parte delle sessioni web dei vostri utenti è attualmente crittografata con il protocollo SSL/TLS (Secure Sockets Layer/Transport Layer Security) o HTTPS. Questo perché il settore oggi mostra una massiccia tendenza a prediligere un Internet totalmente criptato per centrare due obiettivi fondamentali:

- rendere più difficile ai criminali informatici intercettare le connessioni web
- tenere al sicuro e riservate le informazioni personali

Poiché il traffico "normale" si affida in misura crescente ai protocolli crittografici, la crittografia è divenuta uno dei vettori di minacce prediletti degli hacker per mascherare i propri attacchi, eludere i sistemi di difesa e installare backdoor direttamente nelle reti delle aziende. In fondo, i sistemi di sicurezza aziendali non possono certo bloccare ciò che non riescono a rilevare. In assenza di un intervento efficace, qualsiasi attacco basato sul protocollo SSL/TLS è in grado di mettere a rischio una rete aziendale, con la conseguente perdita di reputazione, IP e dati riservati.

La crittografia è ovunque

Il protocollo SSL/TLS è ormai utilizzato per ogni cosa, dal commercio elettronico ai servizi di banking online. L'SSL/TLS protegge una quantità crescente di traffico aziendale e costituisce la maggior parte del traffico di rete in alcuni sistemi verticali. L'SSL protegge i dati in movimento creando un canale cifrato al di sopra delle reti private o delle reti Internet pubbliche, un canale che impedisce l'acquisizione o la compromissione dei dati.

Inoltre, il protocollo SSL verifica che i dati non siano destinati a un hacker che sta simulando una destinazione fidata. I dati sensibili e cruciali, come quelli relativi a carte di credito, nomi utente e password, vengono trasmessi in modo tale da rendere difficile a chiunque - tranne che al destinatario prestabilito - accedere a quei dati. Se originariamente gli utilizzatori dell'SSL erano siti web e server Telnet ed FTP, oggi questo protocollo è utilizzato da una grande varietà di applicazioni, tra cui quelle basate su Java, i servizi di gestione delle applicazioni e servizi cloud-based. Facebook e Twitter sono due delle applicazioni con abilitazione SSL più note e diffuse. Sono inoltre disponibili degli add-on per browser che possono imporre l'uso dell'SSL tramite HTTPS.[1]

Le tradizionali soluzioni di sicurezza per la rete non hanno la capacità di esaminare il traffico SSL/TLS crittografato, oppure le loro prestazioni sono così limitate da renderle inutilizzabili in fase di analisi.

Nel quarto trimestre del 2015 le connessioni HTTPS (SSL/TLS) hanno rappresentato una media del 64,6% delle connessioni web, sorpassando la crescita dell'HTTP per gran parte dell'anno. A gennaio 2015, le connessioni HTTPS hanno superato del 109% quelle di gennaio 2014. Ogni mese del 2015, inoltre, si è registrato un aumento medio del 53% rispetto allo stesso mese dell'anno precedente.

I firewall possono avere difficoltà ad esaminare il traffico crittografato

Mediante la crittografia SSL/TLS gli hacker più esperti possono cifrare le comunicazioni di comando e controllo e i codici dannosi per eludere i sistemi di prevenzione delle intrusioni (IPS) e di ispezione anti-malware. Questi attacchi possono essere estremamente efficaci per il semplice fatto che gran parte delle organizzazioni non dispone di un'infrastruttura adeguata per rilevarli. Le tradizionali soluzioni di sicurezza per la rete non hanno la capacità di esaminare il traffico SSL/TLS crittografato, oppure le loro prestazioni sono così limitate da renderle inutilizzabili in fase di analisi. L'ispezione del traffico HTTPS tramite un firewall di nuova generazione (NGFW) richiede sei processi di elaborazione in più rispetto all'esame del traffico di solo testo.

I due processi che influiscono maggiormente sulle prestazioni sono:

- stabilire una connessione sicura
- decrittografare e crittografare di nuovo il traffico per scambiare dati in sicurezza

In alcuni casi ciò può penalizzare fortemente le prestazioni, fino a impedire l'analisi SSL/TLS nelle aziende che utilizzano sistemi di sicurezza legacy.

Numerosi attacchi informatici sono dettati da motivi opportunistici e la maggior parte di essi da motivi finanziari. Quindi tutte le organizzazioni sono esposte a questo rischio.

Possibili conseguenze per le organizzazioni

Nel corso di quest'anno gli aggressori hanno sfruttato appieno i vantaggi legati all'aumento del traffico HTTPS e la mancanza di visibilità. Un attacco ha utilizzato una pubblicità su Yahoo esattamente in questo modo, esponendo ad un malware ben 900 milioni di utenti. Questa campagna reindirizzava i visitatori di Yahoo a un sito infettato dall'exploit kit Angler. Altri 10 milioni di utenti hanno probabilmente riscontrato un problema simile nelle settimane precedenti accedendo a pubblicità collocate da una società di marketing di nome "E-planning".

Conclusioni

La crittografia è utilizzata ovunque e ora è divenuta uno dei vettori di minacce preferiti dagli hacker. È quindi indispensabile che il vostro sistema di sicurezza sia in grado di decrittografare il traffico per bloccare le minacce nascoste.

Per saperne di più, leggi il nostro documento "Best practice per bloccare le minacce crittografate".

[1] *UBM Tech E-paper: Sicurezza di nuova generazione*

© 2016 SonicWall Inc. TUTTI I DIRITTI RISERVATI.

SonicWall è un marchio o marchio registrato di SonicWall Inc. e/o delle sue affiliate negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi e marchi registrati appartengono ai rispettivi proprietari.

Le informazioni contenute nel presente documento si riferiscono ai prodotti di SonicWall Inc. e/o delle sue affiliate. Né il presente documento né la vendita di prodotti SonicWall costituiscono alcuna licenza, espressa o implicita, di estoppel o di altro tipo, né garantiscono diritti di proprietà intellettuale. SALVO QUANTO SPECIFICATO NEI TERMINI E NELLE CONDIZIONI STABILITI NEL CONTRATTO DI LICENZA DI QUESTO PRODOTTO, SONICWALL E/O LE SUE AFFILIATE NON SI ASSUMONO ALCUNA RESPONSABILITÀ ED ESCLUDONO GARANZIE DI QUALSIASI TIPO, ESPLICITE, IMPLICITE O LEGALI, IN RELAZIONE AI PROPRI PRODOTTI, INCLUSE, IN VIA ESEMPLIFICATIVA, QUALSIASI GARANZIA IMPLICITA DI COMMERCIABILITÀ, IDONEITÀ A SCOPI SPECIFICI O VIOLAZIONE DI DIRITTI ALTRUI. SONICWALL E/O LE SUE AFFILIATE DECLINANO OGNI RESPONSABILITÀ PER DANNI DI QUALUNQUE TIPO, SIANO ESSI DIRETTI, INDIRETTI, CONSEQUENZIALI, PUNITIVI, SPECIALI O INCIDENTALI (INCLUSI, SENZA LIMITAZIONI, DANNI PER MANCATO GUADAGNO, INTERRUZIONI DELL'ATTIVITÀ O PERDITE DI DATI) DERIVANTI DALL'UTILIZZO O DALL'IMPOSSIBILITÀ DI UTILIZZARE IL PRESENTE DOCUMENTO, ANCHE NEL CASO IN CUI SONICWALL E/O LE SUE AFFILIATE SIANO STATE AVVERTITE DELL'EVENTUALITÀ DI TALI DANNI. SonicWall e/o le sue affiliate non rilasciano alcuna garanzia o dichiarazione relativamente alla precisione o completezza dei contenuti del presente documento e si riserva il diritto di apportare modifiche, in qualsiasi momento e senza preavviso, alle specifiche e alle descrizioni dei prodotti. SonicWall Inc. e/o le sue affiliate non si assumono alcun impegno di aggiornare le informazioni contenute in questo documento.

Informazioni su SonicWall

Da oltre 25 anni SonicWall è il partner di fiducia nel campo della sicurezza. Dalla sicurezza della rete alla protezione degli accessi fino alla sicurezza dell'email, SonicWall ha costantemente ampliato la sua gamma di prodotti consentendo alle organizzazioni di fare innovazione, accelerare e crescere. Con oltre un milione di dispositivi di sicurezza in quasi 200 paesi e aree del mondo, SonicWall permette ai suoi clienti di guardare al futuro con fiducia.

Per qualsiasi domanda sul possibile utilizzo di questo materiale, contattare:

SonicWall Inc.
5455 Great America Parkway,
Santa Clara, CA 95054

Consulta il nostro sito Web per informazioni sulle sedi regionali e internazionali.
www.sonicwall.com

© 2017 SonicWall Inc. TUTTI I DIRITTI RISERVATI. SonicWall è un marchio o marchio registrato di SonicWall Inc. e/o delle sue affiliate negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi e marchi registrati appartengono ai rispettivi proprietari.

SolutionBrief-DarkSideOfEncryption-EU-IMAG-22649