SONICWALL®

SCONFIGGERE LE MINACCE CRITTOGRAFATE

Lo stato attuale del traffico crittografato

Gli hacker hanno affinato le proprie abilità nell'utilizzo del traffico SSL per celare gli attacchi e i malware in modo da non essere rilevati dai sistemi di sicurezza.

97% delle imprese intervistate ha notato un aumento del traffico web crittografato[1]

130% di incremento delle minacce che sfruttano connessioni TLS/SSL (nel 2016 rispetto al 2014)[1]

41% del malware viene nascosto nel traffico SSL[2]

80% degli intervistati ha subito un attacco informatico[2]

[1] *Studio di ricerca, NSS Labs, Giugno 2016*
[2] *Studio di ricerca, Ponemon, 2016*

Come funziona l'uso illecito della crittografia

Visita di una pagina: il computer dell'utente (vittima A) accede a un sito benevolo ma compromesso.

Esecuzione dell'exploit kit: mentre il contenuto web viene mostrato all'utente, un piccolo software viene scaricato nel suo dispositivo, dove viene eseguita una sequenza di comandi per sfruttare eventuali vulnerabilità del software.

Richiesta del malware: una volta che l'esecutore dell'exploit kit ha assunto il controllo del dispositivo, viene inviato un comando di richiesta al sito web che ospita il malware in modo che questo sito invii il malware.

Infezione da malware: ora il malware si è installato nel dispositivo della vittima A.

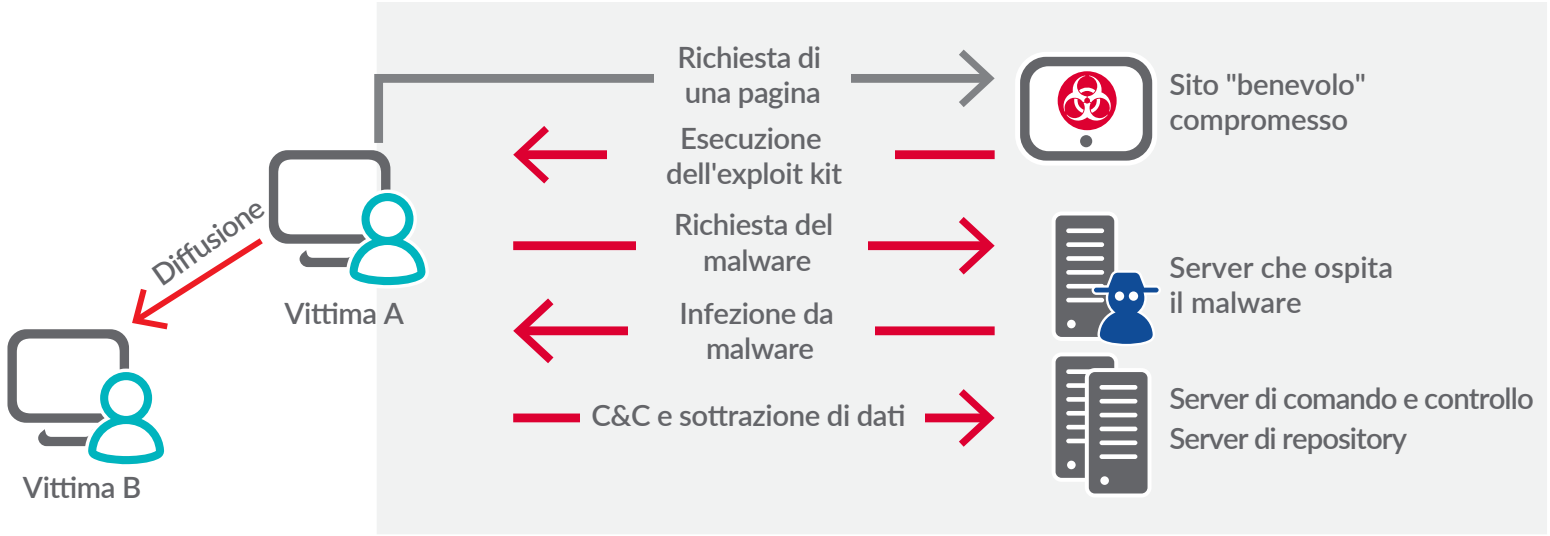
Comando e controllo (C&C): il malware comunica con l'infrastruttura di comando e controllo per richiedere ulteriori istruzioni.

Sottrazione dei dati: i dati del dispositivo della vittima A vengono copiati su un server esterno per essere poi elaborati.

Vittima B: a questo punto, spesso gli aggressori aumentano i propri diritti di accesso in modo da muoversi orizzontalmente all'interno della rete e infettare altri terminali.

Crittografia: la novità sta nel fatto che ora la crittografia è implementabile in qualunque fase di questo attacco per evitare il rilevamento.

La crittografia è implementabile in qualunque fase di un attacco



SONICWALL

Le sfide del traffico crittografato

I tre fattori principali che ostacolano l'ispezione del traffico SSL

Mancanza di strumenti di sicurezza efficaci

Risorse insufficienti

Peggioramento delle prestazioni

Fonte: Studio di ricerca, Ponemon, 2016

SONICWALL®

L'impatto sulle prestazioni è una delle principali preoccupazioni

- Con le funzioni d'ispezione del traffico SSL attive, le prestazioni di un sistema di sicurezza possono peggiorare anche dell'**81%**[1]

- Il **61%** dichiara che un calo di prestazioni è il timore principale delle aziende che non decrittografano il traffico SSL[2]

- L'**83%** afferma che la decrittografia genera un calo di prestazioni nelle aziende che attualmente adottano protocolli di decrittografia e ispezione del traffico SSL[2]

[1]*Fonte: SSL Performance Problems NSS Labs, Giugno 2013*
[2]*Fonte: Studio di ricerca, Ponemon, 2016*

Tre domande difficili ma indispensabili

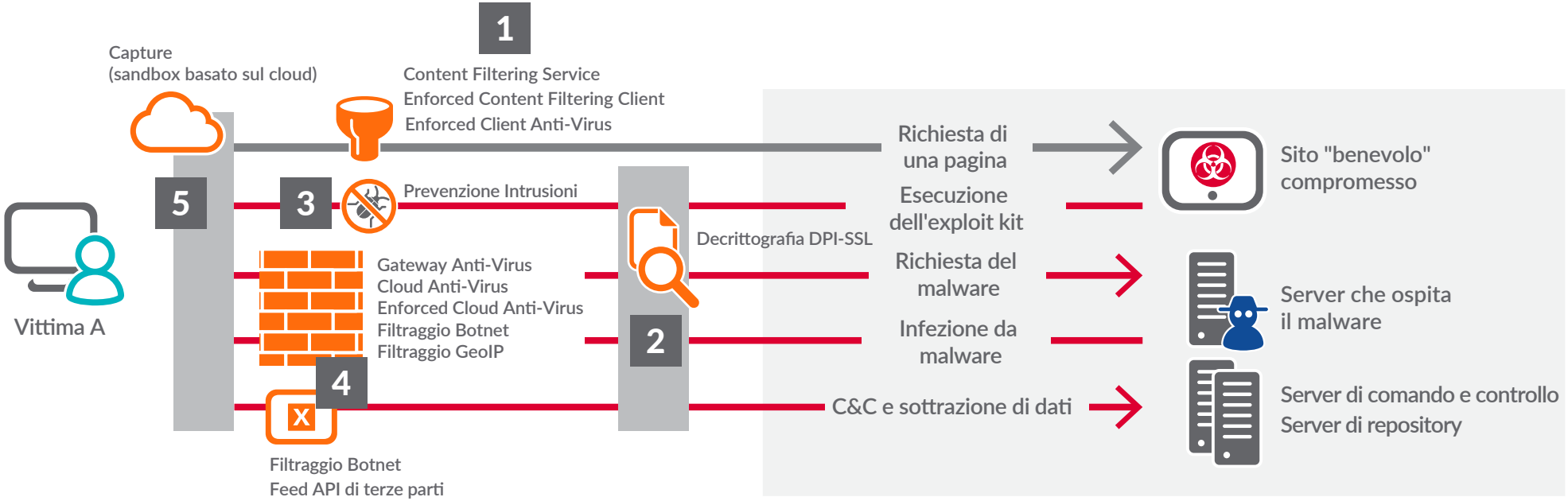
Ecco tre domande difficili che ti DEVI porre relativamente al traffico SSL crittografato:

- Sai se il firewall della tua azienda ispeziona il traffico HTTPS?
- La tua organizzazione ha avuto frequenti interruzioni del servizio di rete o downtime a causa di un crollo totale delle prestazioni del firewall durante l'ispezione del traffico HTTPS?
- Come gestisci la protezione del firewall per evitare cali di prestazione, lentezza e latenza della rete durante l'ispezione del traffico HTTPS?

La soluzione SonicWall

La soluzione SonicWall: spezzare il ciclo del malware che opera nel traffico crittografato

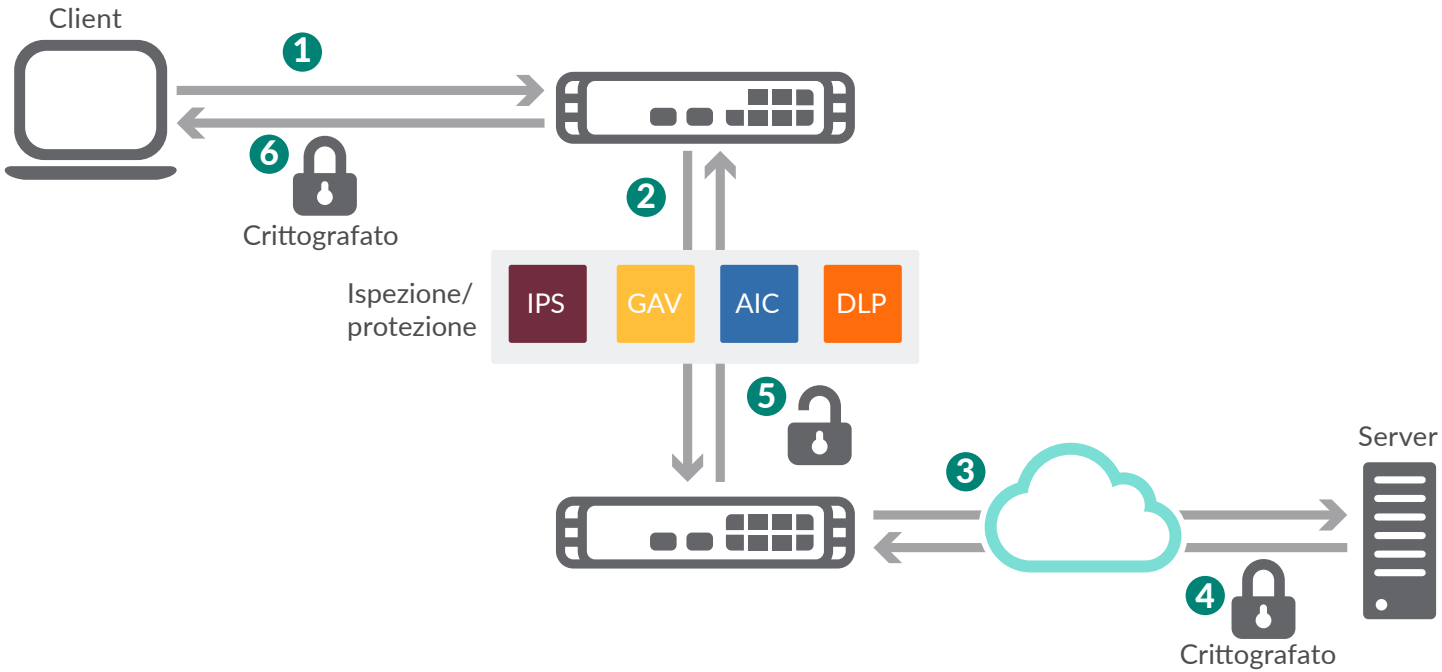
1. SonicWall protegge i sistemi endpoint all'interno e all'esterno del perimetro del firewall impedendo l'accesso a URL inappropriati, illegali e dannosi mediante le soluzioni Web Content Filtering e Enforced Content Filtering Client del firewall.
2. L'esclusiva tecnologia d'ispezione Deep Packet del traffico SSL (DPI-SSL) di SonicWall decripta il traffico internet crittografato tra i client e i server web.
3. Il servizio di prevenzione delle intrusioni SonicWall analizza il traffico non crittografato, fornendo protezione da vulnerabilità delle applicazioni e da worm, Trojan, exploit peer-to-peer, spyware e backdoor exploit.
4. I servizi di prevenzione delle minacce SonicWall quali Gateway Anti-Virus, Cloud Anti-Virus, Filtraggio Botnet e GeoIP, abbinati alle informazioni sulle minacce di fornitori esterni, contribuiscono a interrompere il ciclo dell'infezione malware.
5. SonicWall Capture ATP, una piattaforma sandbox multi-engine, esegue ed esamina i file sospetti per rilevare e bloccare eventuali minacce zero-day.



SONICWALL®

La soluzione SonicWall: decrittografia e ispezione del traffico crittografato tramite DPI-SSL

1. Il client avvia il processo di handshake SSL/TLS con il server
2. Il firewall NGFW intercetta la richiesta e stabilisce una sessione utilizzando i propri certificati al posto di quelli del server
3. Il firewall NGFW inizia l'handshake SSL/TLS con il server per conto del client, utilizzando il certificato SSL/TLS definito dall'amministratore
4. Il server completa l'handshake e crea un tunnel sicuro tra sé e il firewall NGFW
5. Il firewall NGFW decripta e ispeziona tutto il traffico proveniente da o diretto al client, alla ricerca di minacce crittografate
6. Il firewall NGFW ricodifica il traffico sicuro, lo invia al client e blocca le minacce crittografate



SONICWALL®

I vantaggi per il cliente

- Maggiore visibilità nel traffico SSL/TLS crittografato
- Blocco di download di malware nascosti nel traffico crittografato
- Contrasto alle comunicazioni di comando e controllo (C&C) e alla sottrazione di dati
- Miglioramento delle funzioni di sicurezza, controllo delle applicazioni e prevenzione di perdite di dati
- Massimo sottrazione di dati livello di qualità del servizio e disponibilità della rete e delle risorse, senza problemi di prestazioni, man mano che aumenta il carico del sistema

Per saperne di più: visita www.sonicwall.com/encrypted-threats.

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