SONICWALL®

IL LATO OSCURO DELLA CRITTOGRAFIA

Gli hacker hanno aumentato le loro capacità di utilizzare il traffico SSL per celare i loro attacchi e malware ai sistemi di sicurezza.

97% delle imprese intervistate vedono un aumento del traffico web criptato[1]

130% di aumento delle minacce che utilizzano connessioni TLS/SSL nel 2016 rispetto al 2014[1]

80% degli intervistati sono stati vittime di un attacco informatico[2]

41% degli attacchi erano nascosti nel traffico SSL[2]

[1] *Research Study, NSS Labs, giugno 2016*
[2] *Research Study, Ponemon Study 2016*

SONICWALL®

Gli attacchi che sfruttano il traffico SSL per eludere il rilevamento

Attacco nascosto nel traffico «normale» della porta 443

- Il 78% pensava che la loro attività sarebbe stata presa di mira probabilmente.
- Meno di un terzo (30%) delle attività aveva fiducia nella propria capacità di risolvere il problema.

Phishing

- Il 79% ritiene molto probabile che questo problema possa verificarsi nella loro attività.
- Solo il 17% afferma che la propria attività sia in grado di mitigare un tale attacco.

Malware che nasconde dati in uscita nel traffico crittografato

- Il 74% ammette che questo vettore d'attacco è altamente probabile.
- Solo il 16% afferma che la propria attività potrebbe identificare e mitigare l'attacco malware crittografato in SSL prima della fuoriuscita dei dati.

Il responsabile dell'attacco potrebbe nascondere i dati in uscita e/o rubati verso un server di comando e controllo

- Il 66% afferma che la probabilità di un evento di questo tipo è elevata.
- Il 26% crede che la propria attività potrebbe individuare questo comportamento e impedire la perdita dei dati.

Research Study, Ponemon Study 2016

SONICWALL®

Comprendere l'uso dannoso della crittografia

Richiesta di pagina: la macchina utente (vittima A) visita un sito affidabile ma compromesso.

Esecuzione di un kit di exploit: quando il contenuto web viene fornito al client, viene scaricato un piccolo software sul dispositivo dell'utente, in cui viene eseguita una sequenza di comandi per sfruttare le vulnerabilità del software sulla macchina client.

Richiesta malware: una volta che l'operatore del kit di exploit ottiene il controllo di tale macchina, viene inviato un comando di richiesta a un sito web che ospita il malware e che consegna il malware.

Infezione da malware: il malware è ora installato presso la vittima A.

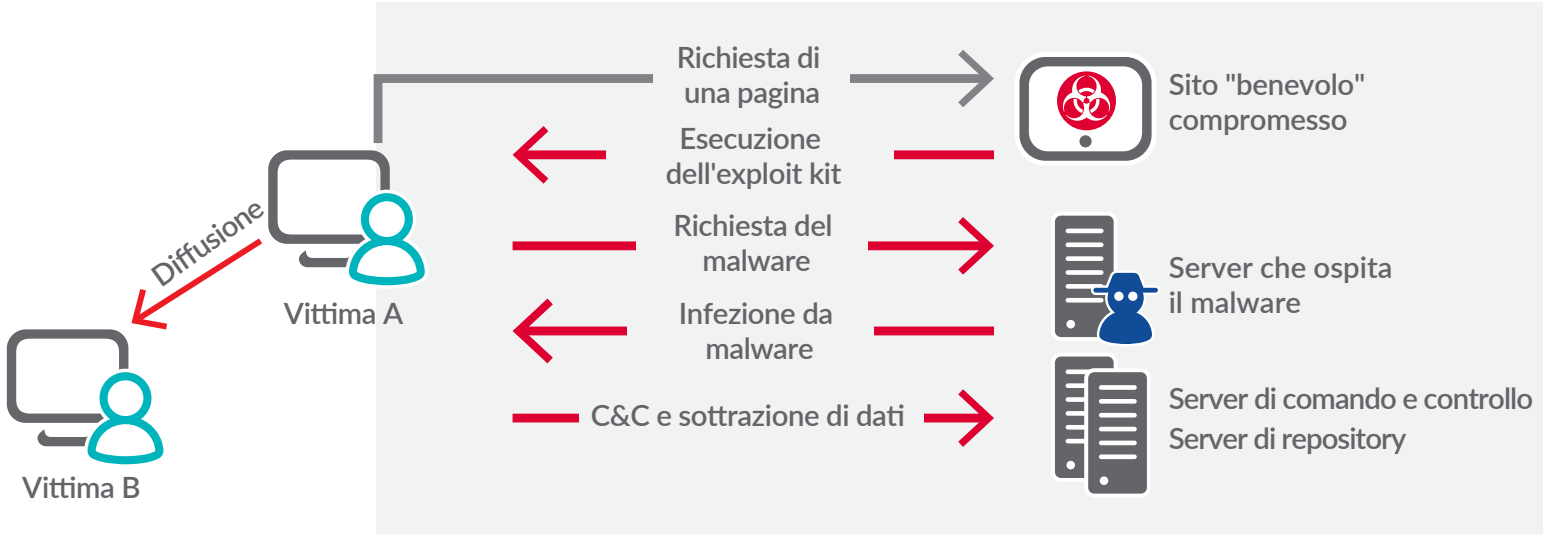
C&C: il malware effettua una comunicazione di ritorno ad un'infrastruttura di Comando e Controllo per ulteriori istruzioni.

Fuoriuscita dei dati: i dati provenienti dalla macchina della vittima A vengono copiati su un server esterno per l'elaborazione.

Vittima B: a questo punto, gli aggressori aumentano spesso i propri diritti di accesso consentendo loro di muoversi lateralmente all'interno della rete e infettare altri endpoint.

Crittografia: la realtà odierna è che la crittografia può essere implementata in qualsiasi fase di questo attacco per eludere il rilevamento.

La crittografia può essere implementata in qualsiasi fase di un attacco



SONICWALL

Tre barriere comuni alla mancata ispezione del traffico SSL

Mancanza di strumenti di sicurezza efficaci

Risorse insufficienti

Degrado delle prestazioni

Fonte: Research Study, Ponemon Study 2016

SONICWALL®

L'impatto sulle prestazioni è una grande preoccupazione

- **61%**: percentuale di coloro per cui le prestazioni insufficienti preoccupano le attività che non decrittano il traffico SSL*
- **83%**: percentuale di coloro per cui la decrittazione produce un qualche tipo di degrado all'interno delle attività che eseguono attualmente la decrittazione e l'ispezione del traffico SSL*

**Fonte: Research Study, Ponemon Study 2016*

Alcune domande scomode

- Sapete se il firewall della vostra attività ispeziona il traffico HTTPS?
- La vostra attività ha subito frequenti interruzioni del servizio di rete o downtime a seguito di un crollo totale delle prestazioni del firewall durante l'ispezione del traffico HTTPS?
- Come state affrontando la scalabilità della protezione firewall per impedire il degrado delle prestazioni, il lag ritardo e la latenza della rete durante l'ispezione del traffico HTTPS?

Consigli

- Se da tempo non effettuate una verifica della sicurezza, è giunto il momento di intraprendere una valutazione completa della sicurezza di rete per identificare i vostri rischi e le vostre esigenze.
- Aggiornate le vostre politiche di sicurezza per difendervi da una vasta gamma di vettori di minacce e stabilite numerosi metodi di difesa di sicurezza per rispondere agli attacchi provenienti dal traffico HTTP o HTTPS.
- Implementate un firewall di nuova generazione con funzionalità di ispezione Secure Sockets Layer/Transport Layer Security (SSL/TLS) ad alte prestazioni. Assicuratevi di poter ispezionare tutto il traffico indipendentemente dalle porte, dai protocolli o dalle dimensioni dei file, decomprimendo e decrittando ogni pacchetto ed esaminando ogni byte per identificare rapidamente le minacce.
- Le soluzioni di sandboxing standard non catturano il malware nascosto nel traffico crittografato. L'ispezione SSL/TLS è una necessità, così come una sandbox di rete che blocchi il traffico fino a raggiungere un verdetto e che non si limiti a individuare gli attacchi zero-day, ma sia in grado di prevenirli in modo automatizzato.
- Aggiungete il filtraggio dei contenuti per impedire agli utenti di visitare siti dubbi e di utilizzate un sistema antivirus e di prevenzione delle intrusioni al gateway per proteggerli dai siti «buoni» compromessi.
- Implementate una formazione continua affinché il vostro personale sia consapevole del pericolo dei social media, dell'ingegneria sociale, dei siti web sospetti e dei download, nonché dei vari spam e scam di phishing. E soprattutto informate gli utenti di non accettare mai un certificato autofirmato e non valido.
- Assicuratevi di una buona igiene informatica e accertatevi che tutti i vostri software siano aggiornati con tutti gli aggiornamenti della protezione. In questo modo potrete proteggere tutte le macchine dagli exploit SSL più vecchi e già neutralizzati.
- Stabilite e sperimentate la vostra reazione e il piano di remediation. Testate regolarmente il vostro piano, eseguite delle simulazioni come se fossero esercitazioni antincendio, migliorate il processo e fate in modo che i primi a reagire siano più efficienti e ben addestrati per eseguire i piani di remediation secondo il progetto

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 eventuali domande in merito all'utilizzo potenziale del presente materiale, si prega di contattare:
SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Per maggiori informazioni, visitare il nostro sito web.
www.sonicwall.com