Panoramica sulla soluzione

Blocco dell'esfiltrazione dei dati

Proteggi i gioielli della corona.

Nel **Report McAfee® Labs sulle minacce: agosto 2015**, prediamo approfonditamente in esame uno dei passaggi chiave del processo del furto di dati: l'esfiltrazione dei dati. In base a questo passaggio, il ladro o l'aggressore sposta o copia i dati dalla rete del proprietario a quella controllata dall'autore dell'attacco.

Negli ultimi 10 anni, il settore ha registrato una crescita senza precedenti per violazioni dei dati e per volume di persone e aziende interessate. Le violazioni sono passate dalla raccolta dei numeri di carte di credito e di debito al furto di ogni tipo di informazione immessa online: nomi, date di nascita, indirizzi, numeri di telefono, informazioni sanitarie, credenziali dei conti e molte altre.

Sfortunatamente, non sono i singoli individui le sole vittime. Lo spionaggio informatico esercitato dai governi, dalle organizzazioni criminali e dagli attivisti informatici ha messo ovunque a rischio i dati sensibili di persone e aziende.

Autori delle minacce e motivazione

Un autore delle minacce è una persona o un gruppo che tenta di ottenere l'accesso non autorizzato alle reti e ai sistemi informatici. In tutta la comunità sicurezza, classificare tali minacce equivale a individuare tre principali categorie: governi, criminalità organizzata e attivisti informatici. La tabella seguente ne approfondisce le motivazioni e illustra i tipi di dati considerati potenzialmente preziosi.

	Governo	Criminalità organizzata	Attivisti informatici
Moventi generici	Spionaggio Influenza	Economici	Legati alla reputazione Sociali
Esempi di tipi di dati	Codice sorgente Email Documenti interni Attività militare Informazioni di identificazione personale di funzionari amministrativi	Dati di conti bancari Dati di carte di credito Informazioni di identificazione personale (codici fiscali, dati sanitari)	Email Informazioni sui dipendenti Tutti i dati interni sensibili
Volume dei dati presi di mira	Da piccolo a grande	Grande	Da piccolo a grande
Livello di raffinatezza delle tecniche di esfiltrazione	Elevato	Da medio a basso	Da medio a basso
Posizione dei dati in rete	Sconosciuta/ spesso disseminati	Nota	Sia nota che sconosciuta/ spesso disseminati

intel Security

Obiettivi con dati

Quando un aggressore compromette un sistema all'interno di una rete, avvia l'esplorazione di altri sistemi per scoprire quelli che contengono dati appetibili. Una rete complessa contiene molti tipi di dati e per questo si tratta di un'operazione lunga, per chiunque non disponga di informazioni riservate, che incrementa le possibilità di essere rilevati. Per tale motivo, gli aggressori fanno il possibile per essere il più invisibili e persistenti possibile.

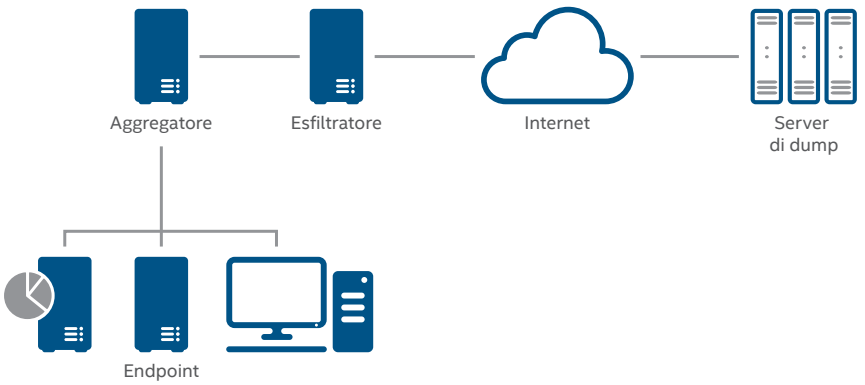
I principali obiettivi con dati sono:

Obiettivo con dati	Tipi di dati	Autori interessati
Sistemi database	Informazioni sanitarie riservate, dati di identificazione personale, carte di credito, dati bancari e account utente	Criminalità organizzata, attivisti informatici
Archivi di codice sorgente	Codice sorgente, credenziali, chiavi	Governi, attivisti informatici
Sistemi specialistici	Variabile	Tutti, a seconda del tipo di endpoint
Sistemi di condivisione file e simili	Codice sorgente, progetti, comunicazioni ecc.	Governi, attivisti informatici
Email e comunicazioni	Progetti, comunicazioni	Governi, attivisti informatici

Esfiltrazione dei dati

Una volta che gli autori delle minacce hanno individuato e ottenuto i dati desiderati, ha inizio l'operazione più difficile del loro compito: l'esfiltrazione del tesoro carpito. Gli autori dell'attacco sfruttano l'ambiente dell'host per agire da intermediari tra le reti della vittima e quelle dell'aggressore. Questa infrastruttura di raccolta può essere semplice o complessa, a seconda di quanto sono profondi o segmentati i dati sulla rete. Alcuni dei ruoli che i sistemi possono adottare nell'infrastruttura di raccolta possono interessare:

- **Endpoint:** uno o più obiettivi con dati sullo stesso segmento dell'aggregatore o su un segmento a esso instradabile.
- **Aggregatore:** funge da punto di raccolta per i dati degli endpoint di riferimento e carica i dati sull'esfiltratore. L'aggregatore può disporre di accesso a Internet, ma non necessariamente. Nelle campagne più sofisticate, più aggregatori possono trasferire dati a svariati esfiltratori per occultare il percorso dei dati in uscita.
- **Esfiltratore:** prende i dati da un aggregatore e ne facilita il trasferimento al server di dump dell'aggressore. Può trattarsi di un semplice trasferimento, oppure l'esfiltratore può ospitare i dati che l'aggressore preleverà.



Tipica architettura di esfiltrazione dei dati.

A prescindere dal fatto che sia un'attività semplice o complessa, l'obiettivo dell'aggressore è spostare i dati presi di mira su un server esterno alla rete della vittima. I server di dump sono i primi punti in cui le informazioni rubate risiedono al di fuori del controllo della vittima e a cui gli aggressori possono accedere liberamente. Tali server possono essere:

- **Sistemi compromessi:** sistemi che sono stati compromessi dall'aggressore durante un'altra campagna. Possono essere sistemi di qualunque tipo, dai blog personali su WordPress ai server aziendali dotati di controlli di sicurezza inefficienti.
- **Sistemi in hosting in paesi specifici:** i paesi con norme restrittive sulla privacy sono interessanti per gli aggressori perché possono ospitare entro i loro confini sistemi che operano indisturbati e con un certo livello di protezione.
- **Sistemi in hosting temporanei:** sistemi dalla vita breve ospitati sul cloud tramite provider come Amazon Web Services, Digital Ocean o Microsoft Azure.
- **Servizi cloud di condivisione file:** siti di condivisione file online accessibili a tutti come DropBox, Box.com e Pastebin.
- **Servizi su cloud:** altri servizi Internet come Twitter e Facebook che consentono agli utenti di pubblicare dati.

Trasporto dei dati

Il trasporto dei dati è costituito dai protocolli e dai metodi utilizzati dai ladri per copiare i dati da una posizione o da un sistema a un altro, sia da interno a interno (da endpoint ad aggregatore) sia da interno a esterno (da esfiltratore a server di dump). Di seguito è riportato un riepilogo di alcuni dei più comuni protocolli di trasporto.

Trasporto	Descrizione	Interno	Esterno
HTTP/HTTPS	La prevalenza del protocollo HTTP nelle comunicazioni in rete lo rende ideale per nascondere i dati esfiltrati in mezzo al resto del traffico. È stato impiegato come trasporto generico per l'esfiltrazione incorporando i comandi nelle intestazioni HTTP e nei metodi GET/POST/PUT.		■
FTP	L'FTP, spesso disponibile sui server aziendali, è un protocollo con cui è facile interagire mediante comandi nativi di sistema ed è quindi un tipo di trasporto che non crea problemi.	■	■
USB	I dispositivi di archiviazione USB sono usati spesso per l'esfiltrazione quando occorre penetrare in reti con accesso circoscritto da air gap. Abbiamo osservato del malware che cerca un dispositivo di archiviazione USB dotato di un marker specifico e, quando lo trova, copia i dati da esfiltrare in un settore nascosto del dispositivo. L'esfiltrazione inizia quando questo viene collegato a un altro sistema infetto dotato di accesso alla rete. I dispositivi di archiviazione USB possono essere utilizzati anche da un insider per copiare facilmente grandi quantità di dati e sottrarli fisicamente all'organizzazione.	■	■
DNS	Record DNS specifici come TXT o persino record A e CNAME possono, in una certa misura, memorizzare dati al loro interno. Con il controllo di un server di domini e di un server dei nomi, un aggressore può trasmettere piccole quantità di dati eseguendo ricerche specifiche sul sistema da cui esfiltrare.		■
Tor	L'uso della rete Tor è sempre più diffuso e permette agli aggressori di inviare i dati esfiltrati a server difficili da rintracciare. Tuttavia, il traffico su Tor nelle reti aziendali raramente è legittimo e quindi è facile da rilevare e da bloccare.		■
SMTP/email	I server SMTP di proprietà della società o di terzi si possono utilizzare per inviare dati all'esterno dell'organizzazione sotto forma di allegati o nel corpo dei messaggi email.		■
SMB	SMB è un protocollo comunissimo negli ambienti Microsoft Windows e in alcuni casi è già abilitato sui sistemi.	■	
RDP	RDP supporta varie operazioni quali il copia/incolla e la condivisione di file, e in alcuni casi i sistemi che consentono l'uso di questo protocollo possono essere a contatto diretto con Internet.	■	■
Protocolli di trasporto personalizzati	Nelle comunicazioni fra i server di controllo e le forme di malware più sofisticate sono spesso utilizzati protocolli di trasporto personalizzati. L'ideazione di un protocollo di trasporto efficace richiede notevoli sforzi e la sua unicità ne facilita l'identificazione in rete, il che fa propendere per l'uso di un protocollo di trasporto standard.	■	■

Manipolazione dei dati

Gli aggressori prendono ogni misura necessaria per assicurarsi di non svelare i loro piani alle vittime quando gestiscono ed esfiltrano dati sensibili. La manipolazione dei dati prima del relativo trasferimento può aiutare a evitare il rilevamento, abbreviare i tempi di trasferimento e persino allungare i tempi di rilevamento. Alcune delle tecniche comunemente viste in questa fase:

Tecnica	Descrizione
Compressione	La compressione con il formato ZIP standard non solo garantisce un certo grado di occultamento ma velocizza il trasferimento dei file.
Divisione in blocchi	La suddivisione dei dati in piccoli blocchi prima dell'invio aiuta a dissimulare il trasferimento fra le normali attività della rete.
Codifica/occultamento	Il tipo più comune di manipolazione dei dati è un algoritmo di codifica o di occultamento di base. Mediante tecniche semplici quali la crittografia con metodo XOR con una chiave statica, la codifica Base64 o la semplice conversione dei singoli caratteri in formato esadecimale i dati possono essere manipolati a sufficienza per evitarne il rilevamento.
Crittografia	È sorprendente che la crittografia non venga utilizzata sempre durante l'esfiltrazione. Forse il motivo è che rallenta le prestazioni, o semplicemente che non è necessaria. Quando viene impiegata, i metodi più comuni sono RC4 e AES.

Cosa può fare Intel Security per aiutarti a proteggerti dall'esfiltrazione dei dati

McAfee DLP Discover

Il primo passo per proteggere correttamente i dati è capire dove risiedano le informazioni e quale sia esattamente la natura di quei dati. **McAfee DLP Discover** protegge contro l'esfiltrazione dei dati tramite la semplificazione di questo passaggio mediante le seguenti funzionalità:

- **Identificazione e controllo delle informazioni sensibili:** inventari e indici si contendono le risorse disponibili tramite la scansione automatica di McAfee DLP Discover, consentendoti di comprendere meglio i tuoi dati sensibili, ovunque essi risiedano. McAfee DLP Discover consente di eseguire le query e l'estrapolazione delle informazioni per scoprire come vengono utilizzate, chi le possiede, dove sono archiviate e dove sono state propagate.
- **Revisione e rimedi alle violazioni:** individua le violazioni al contenuto, registra e genera delle firme e invia notifiche di avviso per proteggere in modo più efficace i dati sensibili. L'integrazione con la gestione dei casi e il flusso di lavoro limita la proliferazione di materiali sensibili.
- **Definizione facile delle policy di protezione:** assicura creazione di policy, reporting e gestione intuitive e unificate per garantire un controllo superiore sulla strategia di protezione delle informazioni.

McAfee DLP Monitor

McAfee DLP Monitor raccoglie, tiene traccia e crea report sui dati in movimento su tutta la rete. È possibile individuare facilmente minacce sconosciute ai dati e adottare azioni volte a proteggerli e destinate a garantire che la tua azienda non subisca la prossima massiva violazione di dati.

- **Esame del traffico di rete:** esamina il traffico di rete più approfonditamente con la scansione dati e le funzionalità di analisi leader del mercato di McAfee DLP Monitor.
- **Identificazione rapida dei dati:** dettaglia rapidamente come vengono utilizzati i dati e dove sono diretti tramite il rilevamento in tempo reale, fornendo le informazioni utili all'azione. McAfee DLP Monitor è in grado di rilevare rapidamente oltre 300 tipi di contenuti su qualsiasi porta o protocollo, assicurandosi che la tua azienda non sia cieca.
- **Analisi scientifiche forensi dettagliate:** conduce l'analisi forense per correlare gli eventi di rischio attuali e passati, individuare le tendenze di rischio e identificare le minacce. McAfee DLP Monitor consente di comprendere rapidamente la situazione e di sviluppare le regole e le policy per affrontarla.

McAfee DLP Prevent

McAfee DLP Prevent protegge contro la perdita dei dati garantendone l'uscita dalla rete solo quando è autorizzata, via e-mail, webmail, instant messenger, wiki, blog, portali, HTTP/HTTPS o trasferimenti via FTP. Essere in grado di identificare e contenere rapidamente i tentativi di esfiltrazione è spesso la differenza che esiste tra mantenere al sicuro i tuoi preziosi dati e finire sulle prime pagine dei giornali.

- **Acquisizione di visibilità sugli incidenti di sicurezza:** offre viste di riepilogo e dettagliate sugli incidenti di sicurezza e sulle azioni di mediazione tramite le viste personalizzate e i rapporti sugli incidenti.
- **Implementazione delle policy in modo proattivo per tutti i tipi di informazioni:** implementa le policy per le informazioni che sai essere sensibili e per le informazioni non ovvie di cui non sei a conoscenza. Con un'ampia gamma di policy integrate, che includono conformità, uso accettabile e proprietà intellettuale, puoi abbinare interi documenti o una loro parte a un set completo di regole al fine di proteggere tutte le informazioni sensibili.

McAfee DLP Endpoint

McAfee DLP Endpoint ti consente di monitorare e prevenire istantaneamente l'esfiltrazione dei dati in sede, fuori sede e nel cloud. Monitora rapidamente gli eventi in tempo reale, applica policy di sicurezza a gestione centralizzata e genera rapporti forensi e di proliferazione dettagliati senza ostacolare le operazioni quotidiane.

- **Migliore supporto alla virtualizzazione:** applica delle policy a livello di singolo utente, per più sessioni e VDI, dando flessibilità e consentendo un controllo migliore del flusso dei dati verso i terminali condivisi.
- **Segnalazione e monitoraggio completi degli incidenti:** raccoglie tutti i dati necessari, come mittente, destinatario, data e ora e prova di rete per analisi, indagine e verifica corrette oltre alla valutazione dei rischi e alla remediation.
- **Console di gestione centralizzata:** si avvale della console di gestione McAfee® ePolicy Orchestrator® (McAfee ePO™) per definire le policy, distribuire e aggiornare gli agenti, monitorare gli eventi in tempo reale e generare i rapporti per soddisfare i requisiti di conformità.
- **Gestione completa dei contenuti:** controlla e blocca i dati riservati copiati su dispositivi USB, drive flash, smartphone e altri dispositivi di archiviazione rimovibili, compresi supporti ottici e copie cartacee. L'integrazione di DLP e gestione dei diritti digitali estende la protezione oltre la tua rete.

McAfee Device Control

McAfee Device Control protegge contro l'esfiltrazione dei dati tramite dispositivi di archiviazione e supporti rimovibili come unità USB, smartphone, CD e DVD. Consente alla tua azienda di monitorare e controllare i trasferimenti di dati da tutti i desktop e laptop, a prescindere dalla relativa posizione, siano essi in sede o fuori sede. McAfee Device Control dispone di funzioni che distinguono contenuti e contesto e sono in grado di bloccare i dispositivi:

- **Gestione completa di dispositivi e dati:** controlla il modo in cui gli utenti della tua azienda copiano i dati su unità USB, smartphone, CD e DVD registrabili e molti altri dispositivi che possono essere sfruttati per l'esfiltrazione dei dati.
- **Controlli granulari:** specificano quali dispositivi possono essere utilizzati, quali dati possono essere copiati nei dispositivi ammessi e impediscono agli utenti di copiare i dati da postazioni e applicazioni specifiche.
- **Funzionalità di reportistica e verifica avanzata:** semplifica la conformità grazie a log dettagliati, a livello di utente e di dispositivo. Dettagli come dispositivo, data e ora e prove dei dati vengono registrati e segnalati facilmente a sostegno delle indagini di verifica e conformità.
- **Gestione centralizzata:** offre monitoraggio degli eventi in tempo reale e gestione centralizzata di policy e incidenti tramite l'integrazione con il software McAfee ePO.

McAfee Next Generation Firewall

Proteggiti contro le esfiltrazioni dei dati o gli attacchi che sfruttano le tecniche di evasione avanzate con **McAfee Next Generation Firewall**. McAfee Next Generation Firewall esegue l'ispezione approfondita dei pacchetti, la normalizzazione dell'intero stack e l'ispezione del flusso dati orizzontale per esporre le anomalie del traffico, come le segnalazioni del malware al suo server di controllo o i tentativi di esfiltrare le informazioni dalla tua rete.

- **Sconfigge le tecniche avanzate di evasione:** utilizza normalizzazione multilivello del traffico, impronte digitali basate sulle vulnerabilità e la relativa associazione indipendente dal protocollo.
- **Rileva l'attività del server di controllo:** usa il rilevamento basato sulla decrittografia e l'analisi della sequenza del messaggio per rilevare l'attività del botnet e del server di controllo.
- **Blocco basato sulla localizzazione geografica:** nega le connessioni in entrata e in uscita con i Paesi che non sono in rapporti d'affari con la tua azienda. Ciò riduce le possibilità di ricezione dei comandi del server di controllo, provenienti da quegli indirizzi IP che non hanno motivo di comunicare con il tuo ambiente.

McAfee. Part of Intel Security.
Via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.intelsecurity.com