Strategie di Difesa Cibernetica: Dai Playbook Statici alla Modellazione Dinamica su Grafi Temporali

Chiappini Mario
Corso di Cybersecurity

4 dicembre 2025

Sommario

Il presente documento analizza l'evoluzione delle strategie di difesa cibernetica, contrapponendo la gestione statica degli incidenti tramite Playbook alla necessità di modelli dinamici per la rilevazione delle anomalie. Vengono esaminate le tecniche di attacco avanzate, come il movimento laterale e le Advanced Persistent Threats (APT), e le vulnerabilità intrinseche dei sistemi (es. Smart Card). Infine, si propone un modello teorico basato su grafi temporali ed entropia per identificare deviazioni comportamentali e attacchi complessi, superando i limiti della semplice analisi statistica del traffico.

1 Introduzione: Il Perimetro e la Superficie d'Attacco

La cybersecurity moderna può essere modellata come un gioco non cooperativo tra attaccante e difensore. Le regole di questo confronto sono dettate da due concetti fondamentali:

- **Perimetro:** L'insieme di tutte le componenti dell'infrastruttura (risorse umane, applicativi, hardware).
- **Superficie d'Attacco:** La totalità dei possibili *access point* sfruttabili per una compromissione.

Mentre il difensore opera spesso vincolato da regole predefinite, il "miglior attaccante" è colui che è in grado di cambiare le carte in tavola durante le varie fasi dell'offensiva, rendendo il perimetro un concetto fluido.

2 Gestione Operativa: Il Playbook

Il *Playbook* rappresenta lo strumento fondamentale per la risposta strutturata agli incidenti. Esso descrive l'insieme delle contromisure da attuare al verificarsi di un *alert* o di un attacco accertato. Le fonti informative che alimentano il playbook includono report ufficiali (dataset pubblici, liste di URL malevoli) e report interni standardizzati.

2.1 Contenimento e Contromisure Attive

All'interno del playbook, le azioni di risposta si dividono in due macro-categorie, spesso svolte in parallelo:

1. **Contenimento:** Azioni volte ad "ammorbidire" il rischio e limitare i danni immediati. Queste decisioni sono tipicamente delegate alla struttura tecnica e ai referenti della protezione.

2. **Contromisura Attiva:** Interventi più radicali che richiedono una piena consapevolezza dell'impatto sul business e sull'operatività (es. isolamento totale di un segmento di rete).

3 Metodologie di Attacco e Anomalie

Gli attaccanti moderni sfruttano tecniche che mirano a eludere i controlli perimetrali classici.

3.1 Movimento Laterale

Il movimento laterale consiste in una serie di azioni apparentemente "legali" che consentono all'attaccante di avvicinarsi progressivamente all'obiettivo (tecnica tipica nei Ransomware). Un esempio di catena di attacco è il seguente:

Click (Phishing) $\rightarrow$ Accesso File Condiviso $\rightarrow$ Registrazione Utente $\rightarrow$ Privilege Escalation

L'obiettivo è rendersi indistinguibile da un utente legittimo mentre si esegue lo *scheme up* verso il target.

3.2 Case Study: Vulnerabilità Smart Card

Un esempio storico di sfruttamento di logiche firmware fallaci riguarda le Smart Card. Sia K la chiave asimmetrica utilizzata per la cifratura interna. Durante l'interrogazione del protocollo $P1$ per una transazione, la memoria fisica allocata era di $2k$ byte, mentre la *challenge* prevista era di $1k$. I primi 100 byte erano riservati ai comandi di esecuzione, i restanti vuoti. Un attaccante, accedendo tramite un server infedele, poteva scaricare un payload malevolo che scriveva nello spazio "vuoto" oltre i comandi legittimi. Poiché il firmware:

1. Era settato per calcolare/validare solo i primi 100 byte;

2. Eseguiva tuttavia le istruzioni sulla lunghezza maggiorata;

L'attacco risultava "legale" ai controlli superficiali, ma eseguiva codice arbitrario (tecnica attribuita a gruppi cinesi).

3.3 APT e WebShell

Le *Advanced Persistent Threats* (APT) prevedono il posizionamento di software su server legittimi, rimanendo silenti per mesi nell'inconsapevolezza della vittima. Spesso utilizzano **WebShell**: piccoli programmi ("uova") agganciati a estensioni browser o HTTP che agiscono come *sniffer*, osservando il traffico e profilando l'infrastruttura. L'anomalia principale generata da una WebShell è un flusso dati non autorizzato (il server che "parla" con l'esterno in modo anomalo).

4 Rilevazione: Dall'Analisi Statistica ai Grafi

4.1 Analisi del Traffico e Machine Learning

Un approccio classico alla difesa è l'analisi della curva gaussiana del traffico server. Si cercano gli *outliers*, ovvero comportamenti che deviano dalla distribuzione normale. Tuttavia, questo metodo presenta criticità:

- **Falsi Positivi:** Picchi di traffico plausibili ma benigni.
- **Attacchi Rapidi:** Se l'attacco provoca una piccola deviazione ma si propaga istantaneamente, il danno avviene prima che la statistica possa rilevarlo come anomalia significativa ("la statistica cancella i passi negativi brevi").

L'utilizzo di algoritmi di **Machine Learning non supervisionato** migliora la capacità di scan e ricerca di anomalie in dataset complessi.

4.2 Modellazione tramite Grafi Temporali ed Entropia

Per superare i limiti statici, il problema viene modellato come un sistema dinamico su grafi. Siano:

- C_1: Il grafo dei contesti legittimi (infrastruttura nota).
- C_2: Il grafo dell'attaccante.

L'attacco si configura come l'aggancio dei nodi di C_2 al grafo C_1. Occupare un nodo di C_1 significa espandere C_2 in quel punto.

4.2.1 L'Entropia come Metrica

Definiamo $E(x_i, y_i)$ come l'entropia associata all'arco tra il nodo x_i e il nodo y_i. L'entropia rappresenta qui il "peso" informativo o la complessità della relazione.

$$E_{tot} = \sum_{(x,y)\in G} E(x, y)$$

Una variazione repentina dell'entropia E che si propaga attraverso i nodi del grafo è un indicatore sufficiente per generare un *alert*. Questo approccio trasforma la rilevazione in un problema di analisi delle variazioni topologiche e informative nel tempo, permettendo di identificare anche attacchi che eludono le soglie statistiche semplici.

5 Conclusioni

La difesa cibernetica richiede un'evoluzione dal semplice utilizzo di playbook reattivi verso modelli predittivi e dinamici. Formalizzare l'infrastruttura come un grafo temporale, dove l'attacco è visto come un'interferenza strutturale misurabile tramite l'entropia, offre una prospettiva promettente per contrastare minacce sempre più sofisticate come le APT e i movimenti laterali occulti.

6 Introduzione esercizio: Dal Playbook alla Dinamica

Mentre il *Playbook* rappresenta la risposta statica e procedurale a un incidente noto, la realtà di un attacco informatico è un processo stocastico che evolve nel tempo. Per catturare questa complessità, non è sufficiente osservare lo stato del sistema in un istante t_0, ma è necessario modellare l'evoluzione delle connessioni nel tempo.

Definiamo il dominio del conflitto come l'intersezione di due grafi: il grafo del contesto legittimo (C_1) e il grafo dell'attaccante (C_2).

7 Formalizzazione del Modello

7.1 Il Grafo Temporale

Sia $G_t = (V, E_t)$ un grafo temporale dove l'insieme dei vertici V è l'unione di tutti i nodi possibili, e l'insieme degli archi E_t varia in funzione del tempo discreto $t \in \mathbb{N}$.

Il sistema globale al tempo t è definito come:

$$G_{global}(t) = C_1(t) \cup C_2(t) \cup E_{cross}(t)$$

Dove:

- $C_1 = (V_1, E_1)$ rappresenta l'infrastruttura bersaglio (nodi statici, connessioni legittime).
- $C_2 = (V_2, E_2)$ rappresenta l'infrastruttura dell'attaccante (C&C servers, nodi compromessi).
- $E_{cross}(t)$ è l'insieme degli archi che connettono nodi di V_2 a nodi di V_1 (l'attacco in corso).

L'obiettivo dell'attaccante è espandere C_2 all'interno di C_1, trasformando nodi $v \in V_1$ in nodi controllati.

7.2 Il "Gioco" Cybernetico

Possiamo modellare l'attacco come un gioco sequenziale tra due giocatori: **Attacker (A)** e **Defender (D)**.

- **Stato S_t:** La topologia del grafo G_{global} al tempo t.
- **Mosse dell'Attaccante (M_A):**

1. *Scan:* Identificare un nodo vulnerabile in V_1.
2. *Exploit:* Creare un arco (u, v) dove $u \in V_2, v \in V_1$.
3. *Lateral Movement:* Creare un arco (v_i, v_j) entrambi in V_1 ma controllato da logiche di A.

- **Mosse del Difensore (M_D):**

1. *Monitor:* Calcolare l'entropia $E(G_t)$.
2. *Contain:* Rimuovere archi sospetti (isolamento).

8 Caso di Studio: C_2 (3 Server) vs C_1 (5 Nodi)

Analizziamo un esempio pratico per visualizzare la propagazione.

Configurazione Iniziale ($t = 0$):

- C_1 (Target): 5 nodi $\{n_1, n_2, n_3, n_4, n_5\}$ connessi in una topologia a stella (server centrale n_1).
- C_2 (Attacker): 3 server $\{s_1, s_2, s_3\}$ (es. Command & Control, Payload Server, Exfiltration Server).

8.1 Fase 1: Infiltrazione (Tempo $t = 1$)

L'attaccante usa s_1 per inviare una WebShell su n_3 (nodo esposto, es. Web Server).

$$E_{cross}(1) = \{(s_1, n_3)\}$$

In questo momento, il grafo C_2 si è "agganciato" a C_1. Il nodo n_3 è ora un punto di contatto.

8.2 Fase 2: Movimento Laterale (Tempo $t = 2$)

L'attaccante, controllando n_3, esegue uno scan interno e trova n_1 (Database centrale). Tenta l'accesso.

$$E_{malicious}(2) = \{(n_3, n_1)\}$$

Questo arco esiste già fisicamente in C_1 (poiché il web server parla col database), ma cambia la natura del flusso.

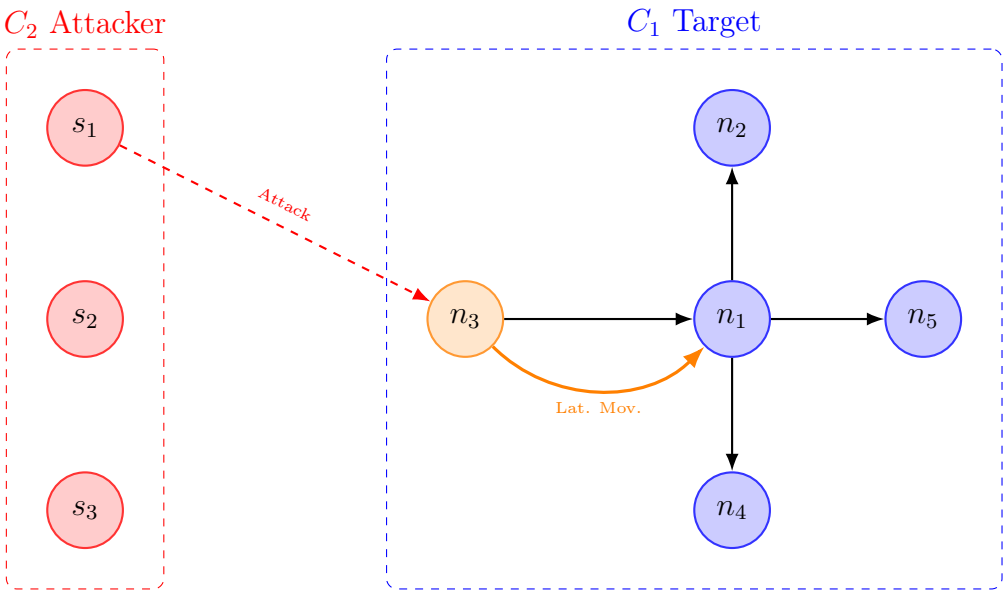

Fig. 1: Rappresentazione dell'aggancio del Grafo C_2 sul nodo n_3 di C_1 e successivo movimento laterale.

9 Rilevazione tramite Entropia

Come distinguiamo l'arco (n_3, n_1) legittimo da quello malevolo al tempo $t = 2$? Utilizziamo l'entropia come misura del disordine o della "sorpresa" nel flusso dati.

Definiamo $P(i, j)$ come la probabilità (basata sullo storico/playbook) che il nodo i comunichi con il nodo j con un certo payload. L'entropia dell'arco è:

$$H(i, j) = -P(i, j) \log_2 P(i, j)$$

9.1 Dinamica dell'Alert

1. **Stato Normale:** Il traffico $n_3 \to n_1$ è costante (query SQL standard). $H(n_3, n_1) \approx k$ (bassa/stabile).

2. **Stato Attacco:** L'attaccante scarica dati in massa o esegue comandi OS. La distribuzione dei pacchetti cambia drasticamente.

3. **Variazione:**
$$\Delta H = |H_{t=2}(n_3, n_1) - H_{t=1}(n_3, n_1)| > \theta$$
Dove θ è la soglia di tolleranza definita nel Playbook.

Se ΔH supera la soglia e questa variazione si propaga (es. n_1 inizia improvvisamente a parlare con n_5 con alta entropia), il sistema dinamico genera un **Alert**.

10 Conclusioni

Modellare la cybersecurity come l'interazione dinamica tra grafi (C_1 e C_2) permette di astrarre il problema tecnico in un problema topologico. L'attacco non è più visto solo come un "malware", ma come un'espansione non autorizzata del grafo C_2 sui nodi

di C_1. L'entropia fornisce la metrica quantitativa per rilevare queste espansioni anche quando le firme statiche (antivirus) falliscono, permettendo l'attivazione tempestiva delle contromisure previste dal Playbook.