

Email Security: Cyber Kill Chain come modello di Difesa

Per comprendere come difendersi da potenziali attacchi malevoli è necessario studiare come questi avvengano. Per fare ciò, esistono diversi modelli, tra questi uno dei più noti ed utilizzati è quello della “**Cyber Kill Chain**” ideato da Lockheed Martin nel 2011.



Figura 2. Cyber Kill Chain

Questo modello descrive in sette fasi, si veda la figura 2, come un attaccante può compromettere un determinato target e di contro anche come identificare e prevenire potenziali attività malevole:

1. **Reconnaissance:** consiste nella raccolta di informazioni tramite tecniche di social engineering e/o OSINT per identificare e selezionare l'obiettivo. Questa fase può avvenire in due modalità:

- **Passiva:** analisi e raccolta di informazioni tramite l'uso di siti web, annunci, Google, Shodan e simili.
- **Attiva:** tramite l'uso di tool per effettuare scansioni dirette sul target (verifica delle porte aperte con i relativi servizi esposti e molto altro). Tra i tool più noti va sicuramente citato Nmap.

L'obiettivo di questa fase è trovare delle vulnerabilità che, potenzialmente, consentiranno agli attaccanti di entrare nella rete. Di contro la cyber defense dovrà occuparsi di mitigare e ridurre la superficie d'attacco utilizzabile dagli attaccanti.

2. **Weaponization:** trovata una vulnerabilità, gli attaccanti creano o cercano un exploit che consenta di sfruttarla.

In questa fase vengono anche individuati possibili malware a supporto dell'attacco. Spesso per guadagnare l'accesso ad un sistema, vengono sfruttati anche gli zero day o vulnerabilità note ma non ancora "patchate" dagli amministratori del sistema.

3. **Delivery:** consiste nella trasmissione dell'exploit individuato all'obiettivo, di seguito alcuni esempi di come potrà essere consegnato:

- Compromissione di un servizio esposto;
- Invio di una mail malevola all'indirizzo della vittima;
- Campagne di Social Engineering;
- Chiavetta USB lasciata nei pressi dell'azienda, ad esempio nel parcheggio;
- Compromissione di siti web terzi, abitualmente visitati dai dipendenti dell'azienda target (tramite l'uso, ad esempio, di attacchi di cross-site scripting (XSS)).

In questa fase, nella cyber defense, è fondamentale adottare un sistema di monitoraggio che consenta di individuare potenziali attività malevole e quindi strutturare un perimetro difensivo che comprenda almeno: firewall perimetrali, IDS/IPS, secure mail gateway, SIEM e un security operation center (SOC) per la gestione dei molteplici alert che verranno generati.

4. **Exploitation:** consiste nello sfruttamento di una o più vulnerabilità da parte dei malware introdotti nel sistema sotto attacco. Tenzionalmente si fa uso anche di tecniche di obfuscation per rendere queste azioni totalmente invisibili ai sistemi difensivi precedentemente elencati.

5. **Installation:** ottenuto l'accesso al sistema gli attaccanti cercheranno di mantenerlo tentando di installare ulteriori malware e backdoors che gli consentiranno successivamente di propagarsi nella rete e di accedere, tramite movimenti laterali, ad utenze con

maggior privilegio.

6. **Command and Control (C2 o C&C)**: in questa fase si tenta di stabilire una comunicazione stabile e duratura con l'obiettivo di utilizzare la macchina infetta. In questa fase un APT consentirà ad esempio di:

- Esfiltrare informazioni sensibili;
- Infettare altre macchine;
- Effettuare “**privilege escalation**” su macchine amministrative;

In queste ultime due fasi, il monitoraggio delle attività sospette lato cyber defense è fondamentale. È molto importante in questo caso, ad esempio, avere sistemi come **UEBA (User and entity behavior analytics)** e regole di **GPO (Group Policy Objects)** che consentano di individuare comportamenti anomali e accessi non autorizzati.

7. **Actions on objectives**: in quest'ultima fase avverrà il vero e proprio attacco al sistema; Questo varierà in base al tipo di attaccante e alle sue motivazioni, ad esempio:

- Finanziarie;
- Politiche;
- Militari;

L'attaccante avrà accesso a informazioni confidenziali e potrà interrompere servizi e/o avere capacità di bloccare l'ordinaria operatività.

In ogni fase del modello, come visto, è possibile individuare delle azioni per mitigare e quindi interrompere la catena d'attacco. Esistono diverse varianti al modello illustrato ma il cui obiettivo è sempre lo stesso; ovvero comprendere il modus operandi dell'attaccante allo scopo di moderare i rischi e quindi “rompere la catena” al fine di interrompere e/o mitigare la minaccia. Questo modello, infine, è anche utilizzato per comprendere al meglio le **TTPs (Tecniche, tattiche e procedure)** di un determinato “Threat actors” e/o

“Malware”. Come visto, la consegna di un malware può avvenire tramite un’email malevola durante la fase di **delivery**.



Questo articolo è stato estratto dal white paper “Email Security: Intelligenza Artificiale, Protocolli e Best Practice Contro gli Attacchi Informatici” disponibile in maniera libera e gratuita al seguente link: <https://www.ictsecuritymagazine.com/pubblicazioni/email-security-intelligenza-artificiale-protocolli-e-best-practice-contro-gli-attacchi-informatici/>

Articolo a cura di **Fabrizio Giorgione**

Profilo Autore



Fabrizio Giorgione è nato a Napoli (NA) nel 1992. Si è laureato in ingegneria informatica presso l’università degli studi del Sannio il 17 dicembre del 2018 con una tesi dal titolo: “Analisi della superficie di un sistema SCADA”. Ha sviluppato, presso il laboratorio ISWATlab, un’applicazione Android denominata “Privacy Guard” la quale valuta il rischio di privacy leakage, ovvero il furto di informazioni, sugli smartphone (http://www.iswatlab.eu/?page_id=499). Ha effettuato il tirocinio presso lo “ZLab” di “Cse Cyber Sec” nell’ambito “SOC”, “Forensic” e “Malware Analysis”. Attualmente lavora presso la società di “NTT DATA” come “Cyber security Analyst” nel SOC di Napoli. Il suo compito è quello di effettuare analisi di log, di malware e di prevenire minacce interne ed esterne alla sua azienda e ai clienti della società. Si è occupato, inoltre, del montaggio e della gestione di sonde IDS/IPS presso Telecom Italia nella sede di Roma (RM).

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/articoli/email-security-cyber-kill-chain-come-modello-di-difesa/>