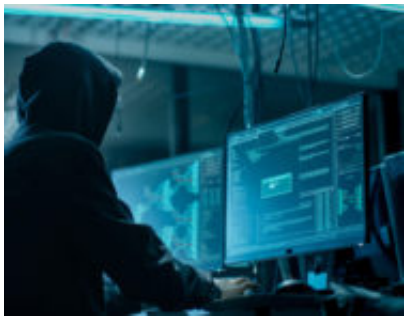
# E se fosse un attacco mirato proprio contro la tua organizzazione? Sapresti gestirlo?

**Author :** Redazione

**Date :** 27 Maggio 2019



Un targeted attack è un attacco organizzato, con un buon livello di pianificazione, rivolto a un obiettivo ben definito (industria, gruppo politico), in prevalenza non automatizzato. E' infatti frequente rilevare dietro le quinte un vero e proprio hacking team dotato di capacità tecniche elevate, evidenziabili dagli indicatori di compromissione/attacco. La parola d'ordine è la seguente: mantenere un basso profilo. Rimanere il più a lungo silenziosi permette di aggirare gli strumenti di difesa dell'azienda oggetto dell'attacco. Per questo motivo si ricorre spesso all'impiego di protocolli di rete legittimi (Adversary OPSEC), frequentemente cifrati. L'obiettivo moderno è il dato, o meglio i Critical-Value Data (CVD), ovvero dati con una rilevanza economica, spendibile sul mercato.

La tempistica prevede spesso tempi medio-lunghi, con uno scenario d'attacco che può delinearsi con ripetuti tentativi nel tempo. Anche gli scopi possono essere svariati: profitto, furto di proprietà intellettuale, vantaggi politici ecc. L'attacco targeted non è mai un "opportunistic attack": non parte da una vulnerabilità per identificare un obiettivo; è semmai vero il contrario.

Se vogliamo tracciare una differenza tra gli attacchi APT (advanced persistent threat) e gli attacchi targeted, possiamo dire che i primi siano sostenuti in linea di principio da una nazione (nation state actor), i secondi da Cyber Criminals più o meno organizzati.

Gli APT impiegano spesso codice sofisticato (le disponibilità finanziaria sono elevate) e 0-day (a dire il vero non sempre necessari). Le motivazioni includono il cyber espionage (furto di segreti industriali, scientifici e tecnologici), ma non esigenze finanziarie immediate (furto di carte di credito, denaro ecc.).  Da non dimenticare che "persistent" significa estrema determinazione: si tratta di una missione che non può fallire e che verrà portata avanti con ogni mezzo possibile. Gli attacchi targeted sono molto diffusi, hanno varie motivazioni, anche economiche. E' prevalente l'impiego di tool open source (anche sofisticati) ed exploit pubblici. Da notare comunque che si delinea sempre di più una linea sottile tra le tecniche utilizzate da entrambe le tipologie d'attaccanti. Le "Tactics, Techniques, and Procedures" (TTP) sono spesso comuni, come sottolinea l'ultimo ENISA Threat Landscape report (gennaio 2019). Si delinea il fenomeno

della "Githubification", ovvero l'impiego di tool open source reperibili su GitHub (Mimikatz, Powersploit, Metasploit, Empire, ad esempio) e la prevalenza di tecniche d'attacco "fileless". L'uso di 0-day (vulnerabilità ancora sconosciute) non è così frequente come si pensi: sono costose da utilizzare, non sempre necessarie. Meglio sfruttare le vulnerabilità dovute ai mancati aggiornamenti, un problema purtroppo diffuso.

I rischi per le aziende sono diversi e dipendono dal settore merceologico d'appartenenza, dalla qualità e dall'importanza dei segreti industriali. Tutte le aziende sono potenziali obiettivi e di questo è bene tenerne conto nella valutazione dei rischi. La buona notizia è che oggi disponiamo degli strumenti per proteggere tutti gli anelli della catena d'attacco (cyber kill chain). Spesso, come rilevato dalla nostra esperienza, si tratta solo di mancanza di volontà e coordinamento da parte delle aziende.

Il Verizon Data Breach Investigations Report (2018) ricorda come nel settore manufatturiero l'86% degli attacchi cyber sia targeted. Il 47% riguarda il furto di proprietà intellettuale al fine di ottenere un vantaggio competitivo e il 66% degli attacchi è stato eseguito con tecniche di hacking avanzate (solo il 34% ha impiegato del malware).

Oltre un terzo di tutti gli incidenti di sicurezza inizia con un'e-mail di phishing o tramite il download di eseguibili dannosi (tecnica di "Drive-by download"). Le tecniche prevedono l'utilizzo di allegati malevoli (eseguibili, PDF, file Microsoft Office, file compressi per celare i contenuti, file *.lnk), oppure il collegamento a file esterni. Le sequenze d'infezione diventano sempre più complesse al fine di aggirare i meccanismi di difesa e prevedono spesso tecniche di persuasione (come la richiesta di decrittare un file per attivare del codice malevolo).

Se è fondamentale che le aziende adottino un metodo "preventivo" per delineare una difesa efficace, il contrasto degli attacchi "targeted" passa necessariamente attraverso un secondo approccio, che potremmo definire di "Detection and Response". In questo contesto entrano in gioco le soluzioni di Managed Detection and Response (MDR).

Si tratta di un servizio gestito focalizzato sulla threat detection, che include un monitoraggio 24x7 da parte di analisti esperti (SOC) al fine di identificare specificamente attacchi targeted utilizzando la telemetria proveniente dagli agenti distribuiti sugli endpoint. Le soluzioni MDR rappresentano un servizio chiavi in mano di Detection e Response, utilizzano la tecnologia del fornitore e si avvalgono di strumenti di Advanced Analytics e Machine Learning. Le aziende clienti hanno in questo modo a disposizione un team di analisti esperti, che spesso include profili diversificati (incident responder, analisti forensi ecc.). Difficile pensare di poter organizzare una linea difensiva così efficare in molti contesti aziendali, anche di grandi dimensioni.

A cura di **Giorgio di Grazia**, Solution Sales Engineer, F-Secure Italy