LUTECH

Le tecniche di attacco "Advanced Persistent Threat"

Stuxnet, Operation Aurora, Red October, Shady RAT, Duqu, APT1, ZeuS e Spyeye, Careto, Snake, Uroburos, Smoke, Turla: una combinazione di minacce informatiche che può essere sconosciuta per chi è estraneo alla sicurezza ICT ma che è in realtà ben nota a chi quotidianamente si occupa delle tematiche relative alla protezione delle informazioni e di risposta agli incidenti di sicurezza. In questo contesto sono saliti alla ribalta della cronaca gli APT (Advanced Persistent Threat), attacchi informatici perpetrati principalmente da agenzie governative e organizzazioni criminali sia per violare le infrastrutture informatiche aziendali ed impossessarsi di dati riservati, identificativi, finanziari e di documenti coperti da proprietà intellettuale e sia con scopi di facile profitto illecito a danno principalmente dei clienti del settore finanziario.

Analizzando il termine APT nei suoi elementi riveleremo tutti gli attributi che caratterizzano l'acronimo:

- **Advanced:** gli attaccanti usano tecniche avanzate con metodologie e strumenti sviluppati ad hoc, sono in grado di combinare molteplici vettori di attacco al fine di raggiungere e compromettere con successo gli obiettivi designati.
- **Persistent:** una volta penetrate le difese, lo scopo dell'attaccante è di mantenere l'accesso rimanendo celato agli occhi della vittima e nascosto agli strumenti di analisi.
- **Threat:** la minaccia è reale, gli attaccanti hanno obiettivi precisi e le capacità tecnologiche e finanziarie per traguardarli. L'attacco viene perseguito e coordinato sfruttando tutte le risorse a disposizione, introducendo così un elemento di massimo rischio nella rete e nei sistemi vittima.

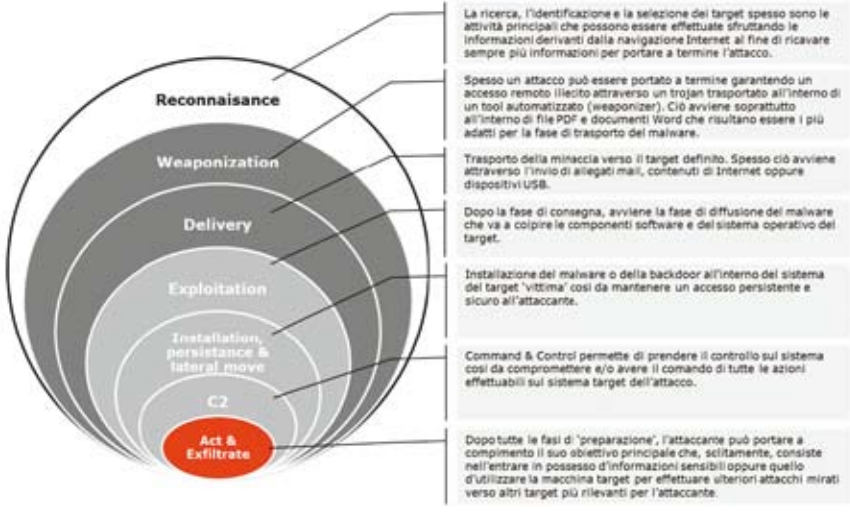
Tutto ciò dimostra come ci sia un alto livello di coordinamento nell'attacco APT e assolutamente non una mera automa-

zione come avviene, invece, nella maggior parte degli attacchi non mirati.

Per maggiore chiarezza sul livello di sofisticazione di un APT, le fasi di un attacco di questo genere, dette anche Cyber Kill Chain, possono essere descritte da sequenze differenti, ognuna rappresentativa di un particolare aspetto:

Dal 2009 ad oggi, alcune delle manifestazioni di APT più note sono state Operation Aurora, Stuxnet, a Lockheed Martin, Telvent, Diginotar, l'APT1, alcune delle Targeted Access Operations della NSA, l'attacco a Target.com. Quanto emerge da questa sintetica sequenza è un quadro preciso sugli APT e sulla loro evoluzione: le prime manifestazioni di questo fenomeno risalgono agli inizi del 2009 e ciò dimostra che nel corso degli anni non sono state messe in campo le corrette

Figura 1 *Cyber Kill Chain*



LUTECH

contromisure, arrivando difatti a sottovalutare la minaccia e il suo impatto reale. Inoltre, si è dimostrato come gran parte di questi attacchi sia stata rilevata con enorme ritardo rispetto all'effettiva compromissione dei sistemi vittima. Analizzando nel dettaglio le manifestazioni di APT elencate, abbiamo anche evidenza di un forte legame tra gli APT e le vulnerabilità Zero Day.

Gli impatti

Nel corso del 2013, gli attacchi APT hanno preso di mira molte nazioni e aziende in tutto il mondo. Di seguito presentiamo una sintesi degli incidenti relativi al 2013:

39.504 Incidenti di sicurezza di cui ➔	4.192 Incidenti di sicurezza riconducibili ad APT
17.995 Infezioni di malware di cui ➔	159 Famiglie di malware associabili ad APT
22 Milioni di comunicazioni verso i Centri di Comando e Controllo in 206 stati	

La sintesi è formulata sulla base di dati che provengono da Threat Intelligence Information Provider estremamente selezionati e specializzati nel monitoraggio avanzato ed integrato tra malware, attacchi mirati e attacchi confezionati sfruttando Zero Day e con visibilità estremamente ampia di tutte le fasi di attacco rappresentate nella Cyber Kill Chain, sia quelle di pre-compromissione ovvero in ingresso, sia quelle di post-compromissione ovvero in uscita. I dati, nello

specifico, provengono da evidenze oggettive di incidenti raccolte sul campo, come già detto a livello mondiale.

Inoltre, dati raccolti a livello mondiale tramite campagne di assessment verticali sul settore finanziario, risalenti all'ultimo quadrimestre 2013 e condotte direttamente sulle infrastrutture di rete dei soggetti analizzati, riportano le seguenti evidenze puntualmente misurate, quindi oggettive:

71 Campagne di misura	99% di soggetti analizzati sono compromessi	10% sono compromessi da un APT

A supporto delle banche, per tener conto dell'evoluzione nelle metodologie di gestione dei rischi, le Nuove Disposizioni di Vigilanza Prudenziale per le Banche emesse da Banca d'Italia con il 15° aggiornamento della Circolare n.263 del 2 luglio 2013 indicano i seguenti requisiti:

- In ambito Funzione di Revisione interna è necessario dare evidenze delle minacce informatiche in evoluzione fornendo strumenti evoluti, al fine di verificare l'adeguatezza, l'affidabilità complessiva e la sicurezza del sistema informativo: la Circolare recepisce in merito (si veda il Par. 3, Sezione III del Titolo V – Capitolo 7) la continua evoluzione delle minacce e la conseguente necessità di contromisure sempre adeguate rispetto a questo contesto dinamico. Gli attacchi APT sono, per la loro natura mirata e sofisticata, la massima esemplificazione di minacce con evoluzione continua.
- In ambito Sistema Informativo occorre ottimizzare i tempi di reazione dei processi di risposta agli incidenti di sicurezza e dotarsi di strumenti oggettivi per valutare e prevenire il rischio informatico: la Circolare in questo punto

recepisce, dato l'aumento del numero di incidenti (tra cui quelli riconducibili ad APT), la necessità di adeguare le capacità di rilevamento e risposta, di conseguenza suggerendo implicitamente (senza entrare nello specifico tecnico si vedano le Sezioni I, II, III e IV del TITOLO V - Capitolo 8) l'esigenza di dotarsi di una maggiore visibilità su tutto l'arco della Cyber Kill Chain, al fine di poter già rispondere agli attacchi anche nelle fasi preliminari.

Le contromisure

Il motivo per cui le comuni tecnologie di difesa risultano inefficaci nella lotta agli APT è da ricercare nel loro funzionamento: molti strumenti, infatti, si focalizzano su porzioni ridotte della Cyber Kill Chain, perdendo così di vista l'intero contesto e tutte le implicazioni dietro ad un determinato evento. Le contromisure più efficienti ed efficaci rispetto agli APT sono strumenti di nuova generazione, le cui caratteristiche principali sono riassumibili come segue:

- La capacità di estendere l'analisi e la copertura rispetto ad un massimo di una o due fasi della Cyber Kill Chain, tipico delle difese tradizionali, ad un approccio senza soluzione di continuità in cui è possibile coprire l'intera catena, permettendo soprattutto di iniziare la risposta all'incidente già dalle sue prime fasi.
- La capacità di identificare i segni di un attacco in modo deterministico ed estremamente chiaro ai fini della massima velocità nella risposta, analizzando il vettore informatico dell'attacco su più livelli (sistemistico, rete, applicativo, etc.), in fasi diverse in modo da scomporne il comportamento nei suoi elementi atomici.
- La capacità di studiare l'attacco non tramite signature o tracce note e neppure tramite il semplice rilevamento

di tentativi di sfruttare vulnerabilità già censite, bensì analizzando il comportamento oggettivo tramite replica dell'esecuzione dei programmi di attacco, con la possibilità quindi di identificare anche fenomeni di attacco che cercano di utilizzare vulnerabilità Zero Day.

- La capacità di ricostruire e analizzare sinteticamente anche attacchi portati in diverse fasi, con diversi vettori, attraverso molteplici canali di ingresso ed uscita.
- La possibilità di arricchire la capacità di rilevamento e di analisi intelligente con informazioni sempre aggiornate e raccolte su scala mondiale.