Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF
Segreteria generale

Centro nazionale per la cibersicurezza NCSC
www.ncsc.admin.ch

NCSC

Minacce generali, autori e strumenti

Indice

1 Premessa

Il documento presenta le ciberminacce più comuni, soffermandosi sulla loro classificazione e sulle tipologie di autore.

2 Minacce

Le minacce provenienti dal web e alle quali sono esposti cittadini, organizzazioni pubbliche e private sono molteplici. Una categorizzazione approssimativa può essere rappresentata con una piramide.

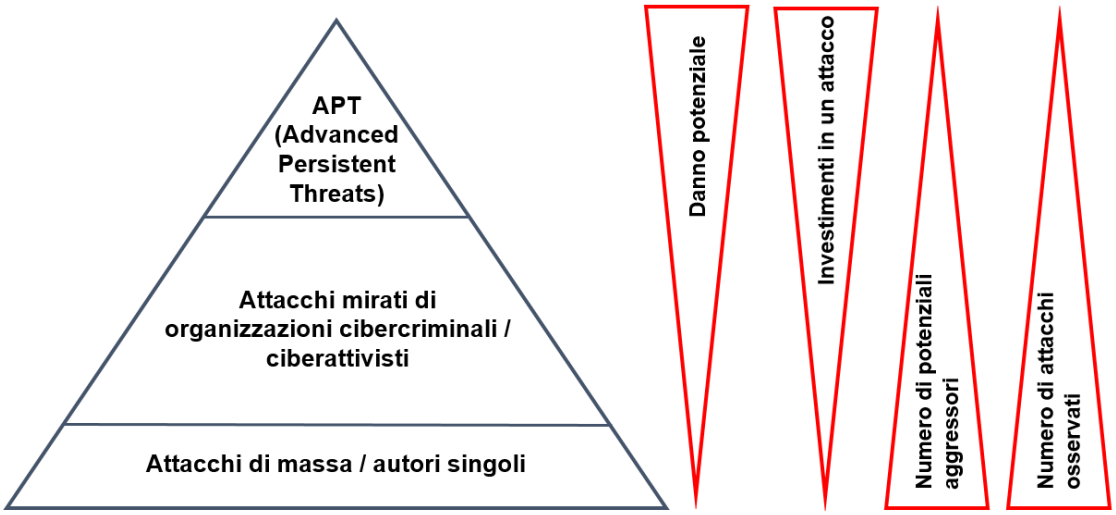

Figura 1: Rappresentazione semplificata delle minacce secondo il SANS Institute[1], «RecordedFuture»[2]

Al vertice della piramide si trovano le minacce persistenti avanzate o APT («Advanced Persistent Threat»). Questo tipo di minaccia può provocare danni molto gravi che si ripercuotono sulla singola organizzazione o, in un contesto politico, sugli interessi di sicurezza di interi Stati. L'aggressore è disposto a investire molto tempo, denaro e conoscenze nell'attacco e dispone generalmente di ingenti risorse. Spesso l'obiettivo dell'aggressore è rimanere nell'ombra il più a lungo possibile e stabilirsi sulla rete della vittima, in modo da sottrarre indisturbato le informazioni che ritiene interessanti. In rari casi si verificano anche (tentativi di) sabotaggi. Poiché sono necessarie risorse e abilità notevoli, il numero di aggressori in questa categoria è limitato, ma in continuo aumento.

Al centro della piramide si trovano le categorie dei cibercriminali e dei ciberattivisti. Sebbene dispongano per lo più di risorse limitate, la minaccia non va sottovalutata. In genere, gli aggressori di questo tipo sono meno selettivi e tenaci rispetto a quelli nella categoria delle APT. Occorre tenere presente che i confini tra cibercriminalità e APT sono labili. Anche gli hacker statali potrebbero approfittare delle offerte del mercato della cibercriminalità per raggiungere gli obiettivi auspicati. Inoltre, gli attori statali ingaggiano anche organizzazioni di cibercriminali per celare le tracce del loro coinvolgimento nel caso in cui l'attacco fosse scoperto.

Alla base della piramide troviamo gli attacchi di massa opportunistici e gli autori singoli. Nonostante le risorse limitate utilizzate per perpetrare queste aggressioni, la minaccia dovrebbe essere presa sul serio per il solo fatto dell'enorme quantità di questo tipo di attacchi. Anche in

[1] www.sans.org

[2] https://www.recordedfuture.com/assets/prioritizing-cyber-threats-1.png

questo caso il confine con il livello superiore non è chiaramente definito, dato che in particolare gli attacchi di massa sovente sono compiuti o commissionati da organizzazioni di cibercriminali. La permeabilità tra i singoli livelli indica pure che il mercato clandestino è organizzato sulla base del classico principio di domanda e offerta.

3 Caratteristiche degli aggressori

Di seguito gli aggressori sono classificati in funzione delle loro possibilità e motivazioni. Questo riepilogo consente di determinare gli obiettivi, le risorse e il grado di tenacia degli aggressori. Si tratta di una classificazione di massima senza pretesa di esaustività.

3.1 APT (minacce persistenti avanzate)

Nome	Attori statali - minaccia persistente avanzata
Descrizione	Stati o attori per lo più con legami statali compiono l'attacco o lo commissionano. In genere questi attacchi sono finalizzati all'ottenimento di informazioni nell'ambito dello spionaggio classico o industriale. In periodi di forte tensione politica o di crisi queste minacce possono anche sfociare in attacchi a infrastrutture critiche o in campagne di disinformazione mirate.
Motivazione	Ottenimento di informazioni, perturbazione delle infrastrutture critiche, persuasione occulta.
Risorse tecniche	È probabile che gli Stati o gli attori con legami statali abbiano tutte le capacità tecniche necessarie. La disponibilità delle risorse deve essere classificata come molto elevata. Inoltre gli specialisti sono disponibili o possono essere reclutati in tempo utile per ogni possibile attività.
Risorse finanziarie	Molto elevate, perlomeno finché secondo l'aggressore il risultato atteso dell'attacco giustifica l'impiego delle risorse finanziarie.
Razionalità del modo di procedere	Elevata
Tenacia	Elevata
Punti di partenza per la difesa	• Investire (anche in termini di personale) nel rilevamento; • aumentare la visibilità dei terminali; • segmentare e sorvegliare le reti e tutti i sistemi; • proteggere le reti Active Directory; • utilizzare strumenti come Applocker e soltanto macro con firma; • impiegare gateway di sicurezza centrali attraverso i quali deve fluire tutto il traffico; • bloccare i tipi di file pericolosi sui gateway; • separare i compiti sensibili dalla navigazione in Internet e dalla posta elettronica; • impostare sistematicamente un'autenticazione a due fattori; • aggiornare i patch regolarmente e sotto sorveglianza; • elaborare un piano di backup e ripristino efficace con backup offline e fuori sede di generazioni diverse.

Punti di partenza per il perseguimento	Effettuare un'analisi dettagliata degli attacchi al fine di permetterne l'identificazione; occorrono indagini coordinate a livello internazionale, che possono essere influenzate da interessi politici.
Capacità di resistenza al perseguimento penale	Molto elevata
Probabili bersagli	• Sistemi con informazioni degne di protezione; • informazioni critiche; • sistemi di persone chiave o decision maker; • accessi secondari a sistemi nascosti che possono essere scoperti difficilmente; • attacchi mirati alla confidenzialità e all'integrità dei sistemi; • attacchi alla disponibilità di sistemi critici in caso di forti tensioni politiche o di crisi; • infrastrutture critiche.

3.2 Organizzazioni cibercriminali – attacchi mirati

Nome	Organizzazioni cibercriminali – attacchi mirati
Descrizione	Le organizzazioni cibercriminali possono eseguire attacchi mirati simili a una APT. Possono attaccare organizzazioni statali o private nell'intento di ottenere informazioni da rivendere o sfruttare a proprio vantaggio. Spesso prendono di mira i sistemi di transazioni finanziarie. Un buon esempio è quello degli attacchi ai bancomat (ATM-Cashout). Per l'aggressore gli attacchi con trojan di crittografia sono molto lucrativi, ragione per cui negli ultimi tempi si osserva una propensione per attacchi di questo tipo. Gli aggressori copiano i dati prima di codificarli e minacciano di venderli se il riscatto non viene pagato.
Motivazione	Estorsione, ottenimento e vendita di informazioni (spionaggio industriale), utilizzo di sistemi di transazioni finanziarie per scopi personali.
Risorse tecniche	Da medie e elevate, a seconda dell'organizzazione.
Risorse finanziarie	Da medie e elevate, a seconda dell'organizzazione.
Razionalità del modo di procedere	Elevata
Tenacia	Media
Punti di partenza per la difesa	• Investire (anche in termini di personale) nel rilevamento; • aumentare la visibilità dei terminali; • segmentare e sorvegliare le reti e tutti i sistemi; • proteggere le reti Active Directory; • utilizzare strumenti come Applocker e soltanto macro con firma; • impiegare gateway di sicurezza centrali attraverso i quali deve fluire tutto il traffico; • bloccare i tipi di file pericolosi sui gateway; • separare i compiti sensibili dalla navigazione in Internet e dalla posta elettronica; • impostare sistematicamente un'autenticazione a due fattori;

	• aggiornare i patch regolarmente e sotto sorveglianza; • Elaborare un piano di backup e ripristino efficace con backup offline e fuori sede di generazioni diverse.
Punti di partenza per il perseguimento	Effettuare un'analisi degli strumenti e dell'infrastruttura di attacco utilizzati, stretta collaborazione con gli organismi di polizia competenti e i servizi delle attività informative. Osservare le organizzazioni cibercriminali in attività.
Capacità di resistenza al perseguimento penale	Da media e elevata Il perseguimento penale ostacola comunque le attività degli aggressori, ragione per la quale essi tentano di rimanere sotto il radar delle autorità di perseguimento penale.
Probabili bersagli	• Sistemi con esigenze di disponibilità elevate; • sistemi con informazioni confidenziali con un elevato valore di mercato; • sistemi con informazioni finanziarie.

3.3 Organizzazioni cibercriminali – attacchi opportunistici

Nome	Organizzazioni cibercriminali – attacchi opportunistici e non mirati
Descrizione	Questa è la forma classica di cibercriminalità. Gli aggressori attaccano il terminale dell'utente finale allo scopo di conseguire un profitto finanziario. Tentano ad esempio di ottenere i dati di accesso, ricattare le vittime tramite attacchi DDoS o inviare spam dai dispositivi infettati. I servizi «Crimeware as a Service», scambiati sul mercato nero, sono spesso utilizzati a tal fine.
Motivazione	Esclusivamente finanziaria
Risorse tecniche	Medie, spesso i componenti per un attacco vengono acquistati sotto forma di «Crimeware as a Service».
Risorse finanziarie	Da medie a elevate
Razionalità del modo di procedere	Elevata
Tenacia	Bassa per i singoli obiettivi
Punti di partenza per la difesa	• Investire (anche in termini di personale) nella sicurezza; • impiegare gateway di sicurezza, bloccare tipi di file pericolosi sui gateway; • separare i compiti sensibili dalla navigazione in Internet e dalla posta elettronica; • impostare un'autenticazione a due fattori per tutte le risorse accessibili da Internet; • aggiornare i patch regolarmente e sotto sorveglianza; • elaborare un piano di backup e di ripristino efficace con backup offline e fuori sede di generazioni diverse.
Punti di partenza per il perseguimento	Utilizzare la tecnica del sinkholing per i domini utilizzati dalle organizzazioni cibercriminali; effettuare un'analisi dell'infrastruttura e degli strumenti di attacco utilizzati; analizzare e impedire i flussi di denaro corrispondenti.
Capacità di resistenza al perseguimento penale	Da media e elevata. La natura internazionale della maggior parte degli incidenti rende più ostacola il lavoro d'indagine.

Probabili bersagli	• Dispositivi di utenti finali scarsamente protetti; • applicazioni di e-banking.

3.4 Hacktivisti

Nome	Hacktivisti - ciberattivisti
Descrizione	I ciberattivisti protestano con mezzi digitali contro le decisioni di Governi o imprese che non collimano con i loro interessi politici e sociali. Esempi di questo tipo i gruppi sono «Anonymous» e «LULZ».
Motivazione	Diffondere messaggi e accendere discussioni, attirare l'attenzione e/o arrecare danni.
Risorse tecniche	Le risorse e capacità tecniche variano fortemente. Le grandi azioni con un grado di attenzione elevato possono richiedere ingenti risorse tecniche.
Risorse finanziarie	Limitate. Tuttavia, questo aspetto non è rilevante poiché in genere l'aggressore aderisce a queste azioni volontariamente.
Razionalità del modo di procedere	Da bassa a media, a seconda della forma organizzativa del gruppo.
Tenacia	Media
Punti di partenza per la difesa	• Investire (anche in termini di personale) nella sicurezza; • impiegare gateway di sicurezza, bloccare tipi di file pericolosi sui gateway; • separare i compiti sensibili dalla navigazione in Internet e dalla posta elettronica; • impostare un'autenticazione a due fattori per tutte le risorse accessibili da Internet; • aggiornare i patch regolarmente e sotto sorveglianza; elaborare un piano di backup e di ripristino efficace con backup offline e fuori sede di generazioni diverse.
Punti di partenza per il perseguimento	Collaborare con gli organismi di polizia e con i servizi delle attività informative.
Capacità di resistenza al perseguimento penale	Media
Probabili bersagli	• Sistemi con grande visibilità/attenzione; • disponibilità dei sistemi (DDoS), integrità («defacement»).

3.5 Autori singoli

Nome	Autori singoli
Descrizione	L'autore singolo agisce per conto proprio con risorse limitate.
Motivazione	Cambia da un individuo all'altro.
Risorse tecniche	Basse
Risorse finanziarie	Basse
Razionalità del modo di procedere	Cambia da un individuo all'altro.
Tenacia	Da bassa a elevata a seconda dell'aggressore.
Punti di partenza per la	• Investire (anche in termini di personale) nella sicurezza;

difesa	• impiegare gateway di sicurezza, bloccare tipi di file pericolosi sui gateway; • separare i compiti sensibili dalla navigazione in Internet e dalla posta elettronica; • impostare un'autenticazione a due fattori per tutte le risorse accessibili da Internet; • aggiornare i patch regolarmente e sotto sorveglianza; • elaborare un piano di backup e di ripristino efficace con backup offline e fuori sede di generazioni diverse.
Punti di partenza per il perseguimento	Normale perseguimento diritto penale
Capacità di resistenza al perseguimento penale	Bassa
Probabili bersagli	• Sistemi scarsamente protetti nel caso di «script kiddie»; • obiettivi ben visibili con grande attenzione in caso di azioni di vendetta («defacement»).

4 Strumenti di attacco

Oltre a una vasta gamma di strumenti che possono essere utilizzati a scopi perfettamente legali (portscanner, «penetration testing tools» ecc.), ne esistono diversi specificamente a scopo criminale. Sono accomunati dal fatto che vengono utilizzati a tutti i livelli della piramide (v. n. 2 «Minacce»).

La banca dati «ATT&CK» di MITRE (https://attack.mitre.org/) offre una panoramica su tattiche, tecniche e procedure adottate per i ciberattacchi.

Per attuarle vengono utilizzati dei malware. MITRE tiene un ampio catalogo di questi parassiti digitali (https://attack.mitre.org/software/).