Gli attacchi informatici spiegati: guida tecnica a come lavorano davvero gli attaccanti

Francesco Barbato · Full Stack · Cybersecurity · AI

Pubblicato il 12 marzo 2026 · 23 min di lettura

SOMMARIO

La maggior parte delle violazioni non parte da un exploit sofisticato: parte da una email di phishing, una password riusata o un server non aggiornato. Un giro tecnico su come funzionano davvero gli attacchi, dal ciclo di vita dell'attaccante e dall'ingegneria sociale a SQL injection, ransomware-as-a-service e compromissioni della supply chain, con casi reali e un modello di difesa a strati.

Parole chiave: Cybersecurity · Hacking · Phishing · Malware · Ransomware · Sicurezza di rete · Sicurezza web · Ingegneria sociale · Supply chain

La cybersecurity non è più un tema solo da reparti IT e specialisti. Riguarda ogni sviluppatore che rilascia codice, ogni manager che approva un acquisto di software, ogni dipendente che maneggia credenziali e ogni dirigente che avalla scelte di infrastruttura. Il panorama delle minacce è maturato, si è professionalizzato ed è cresciuto al punto che l'ignoranza non è più una posizione difendibile per chiunque costruisca o gestisca sistemi digitali.

Questo articolo è un testo tecnico introduttivo: le principali categorie di attacco, come funziona ciascuna a livello meccanico, esempi reali e come appare una difesa efficace. L'obiettivo è la comprensione, non solo il vocabolario.

1 Come ragionano gli attaccanti: il ciclo di vita dell'attacco

Gli attacchi seri, che li conduca uno Stato, un gruppo criminale organizzato o un singolo abile, tendono a seguire un ciclo di vita riconoscibile. Conoscerlo spiega perché nessuna difesa singola basta e perché la difesa in profondità è l'unica strategia coerente.

Il riferimento più usato è il framework **MITRE ATT&CK**, che cataloga tattiche, tecniche e procedure osservate sul campo. Per un'introduzione basta una linearizzazione più semplice:

1. **Ricognizione**: l'attaccante raccoglie informazioni sul bersaglio: nomi di dominio, intervalli IP, nomi ed email dei dipendenti, stack tecnologico, servizi esposti, presenza sui social. Gran parte è passiva e non lascia tracce nei tuoi log.
2. **Accesso iniziale**: il primo punto d'appoggio: una email di phishing che consegna malware, una vulnerabilità sfruttata in un servizio pubblico, credenziali rubate usate su un portale di login o una compromissione della supply chain.
3. **Persistenza**: l'attaccante si assicura di mantenere l'accesso anche se il vettore iniziale viene chiuso: una backdoor, nuovi account utente, script di avvio modificati, infrastruttura di comando e controllo (C2).
4. **Escalation dei privilegi**: passare da un appoggio limitato a privilegi più alti, sfruttando una vulnerabilità locale per diventare root o SYSTEM, abusando di permessi configurati male o rubando credenziali dalla memoria.
5. **Movimento laterale**: muoversi nella rete, compromettere altri sistemi e avvicinarsi ai bersagli di maggior valore.
6. **Esfiltrazione o impatto**: l'obiettivo: rubare dati, installare un ransomware, interrompere le operazioni o stabilire un accesso di spionaggio a lungo termine.

> **IL PROBLEMA DEL DWELL TIME**
>
> Il tempo tra l'accesso iniziale dell'attaccante e la sua scoperta, il dwell time, è calato molto: i rapporti M-Trends di Mandiant indicano una mediana globale di circa 10 giorni per il 2023 (16 l'anno prima), contro più di 200 giorni di un decennio fa. Restano comunque giorni in cui l'attaccante si muove nei tuoi sistemi senza che nessuno se ne accorga. La maggior parte delle difese è pensata per prevenire l'accesso iniziale; molte meno per rilevare e rispondere a un attaccante già dentro.

2 Ingegneria sociale

Le migliori difese tecniche si aggirano telefonando a un dipendente e chiedendogli di reimpostare una password. L'ingegneria sociale sfrutta la psicologia umana invece dei difetti tecnici, ed è costantemente tra i vettori di accesso iniziale più comuni nelle violazioni reali.

2.1 Phishing

Il phishing consiste nell'inviare comunicazioni fraudolente, più spesso email, che sembrano provenire da una fonte fidata, per indurre il destinatario a rivelare credenziali, cliccare un link malevolo o aprire un malware.

Una tipica email di phishing imita un servizio noto (Microsoft, Google, una banca, l'IT interno) e crea urgenza: «Il tuo account è stato compromesso. Verifica la tua identità entro 24 ore.» Il link porta a una copia convincente della vera pagina di login, su un dominio che differisce per un carattere o usa un attacco omografico (una «o» latina sostituita da una «o» cirillica visivamente identica).

L'infrastruttura di phishing moderna è sofisticata. I **kit di phishing adversary-in-the-middle (AiTM)**, come Evilginx2 e Modlishka, funzionano da reverse proxy tra vittima e sito reale: la vittima si autentica sul servizio vero attraverso il proxy dell'attaccante, che cattura il cookie di sessio-

ne in tempo reale, e l'autenticazione a più fattori viene aggirata del tutto, perché la sessione è già autenticata.

2.2 Spear phishing

Il phishing standard è una campagna di massa; lo spear phishing è mirato. L'attaccante studia una persona precisa (ruolo, colleghi, progetti recenti, stile di scrittura) e scrive un messaggio molto personalizzato. Una email che sembra del direttore finanziario e chiede al responsabile dei pagamenti un bonifico urgente è molto più convincente di un generico «il tuo account è bloccato». Lo spear phishing contro amministratori delegati, direttori finanziari e consiglieri si chiama **whaling**: l'impegno è maggiore, e così il guadagno.

2.3 Vishing e smishing

Il **vishing** (voice phishing) usa le telefonate: gli attaccanti si fingono supporto IT, ufficio antifrode di una banca, ente pubblico o un collega. Lo **smishing** (SMS phishing) sfrutta la fiducia maggiore che le persone tendono a dare agli SMS rispetto alle email: un messaggio di un «corriere» con un link di tracciamento o di una «banca» per una transazione sospetta.

2.4 Business Email Compromise (BEC)

La BEC è una frode di ingegneria sociale sofisticata che è costata alle organizzazioni più di ogni altra categoria di crimine informatico: l'FBI riporta oltre 55 miliardi di dollari di perdite nel mondo tra il 2013 e il 2023. L'attaccante prende il controllo di un account email legittimo oppure ne falsifica uno in modo convincente, e lo usa per autorizzare trasferimenti fraudolenti o dirottare pagamenti legittimi.

> **CASO DI STUDIO: L'ATTACCO A TWITTER (2020), INGEGNERIA SOCIALE SU LARGA SCALA**
>
> A luglio 2020 gli attaccanti presero il controllo di account Twitter molto noti, tra cui quelli di Barack Obama, Joe Biden, Elon Musk, Apple e Uber. Non si partì da un exploit tecnico ma da telefonate ai dipendenti: gli attaccanti si finsero il supporto IT interno, ottennero delle credenziali e le usarono per raggiungere gli strumenti di amministrazione interni di Twitter. Da lì presero il controllo degli account bersaglio e pubblicarono una truffa in criptovalute che raccolse circa 120.000 dollari in Bitcoin prima di essere fermata. Furono incriminate tre persone, e il presunto ideatore aveva 17 anni all'epoca. La lezione: nessun irrobustimento tecnico ti protegge da un dipendente che è stato convinto a consegnare i propri accessi.

3 Attacchi alle credenziali

Nome utente e password restano il principale modo di autenticarsi quasi ovunque, e il principale bersaglio degli attaccanti, perché rubare credenziali valide è più facile e più affidabile che sfruttare vulnerabilità.

3.1 Credential stuffing

Sfrutta un'abitudine umana semplice e persistente: il riuso delle password. Quando un grande database di coppie utente-password trapela da un servizio (e miliardi circolano sui mercati clandestini), gli attaccanti usano strumenti automatici per provare le stesse coppie su altri servizi in massa. Una quota rilevante di utenti riusa le password, e l'infrastruttura distribuita permette di provare milioni di coppie in poche ore eludendo rate limiting e blocchi per IP. Strumenti come Sentry MBA, SNIPR e OpenBullet sono software di largo consumo sui forum criminali.

3.2 Password spraying

Il credential stuffing prova molte password su molti account; il password spraying prova poche password comuni («Password1», «Welcome123», «NomeAzienda2024») su un gran numero di account. Resta di proposito sotto le soglie di blocco: invece di martellare un account, fa un tentativo su migliaia di account e poi aspetta prima del successivo. È particolarmente efficace negli ambienti Active Directory con politiche di blocco per singolo account: un tentativo per account all'ora su diecimila account produce moltissimi tentativi senza far scattare nessun blocco individuale.

3.3 Pass-the-hash e pass-the-ticket

Sono attacchi di post-sfruttamento sul livello di autenticazione di Windows. Quando un utente si autentica, l'hash della password o il ticket Kerberos vengono tenuti in memoria dal processo LSASS. Un attaccante con privilegi SYSTEM può estrarli con strumenti come Mimikatz e usarli per autenticarsi come quell'utente su altri sistemi, senza mai conoscere la password in chiaro. Il **pass-the-hash** funziona contro l'autenticazione NTLM, il **pass-the-ticket** contro Kerberos. Entrambi sono standard nel movimento laterale negli ambienti Windows.

> **PERCHÉ L'MFA NON È UNA SOLUZIONE MAGICA**
>
> L'autenticazione a più fattori alza molto il costo degli attacchi alle credenziali, ma non li elimina. Il phishing AiTM la aggira rubando i cookie di sessione dopo l'autenticazione. Lo SIM swapping permette di ricevere i codici via SMS. Gli attacchi di stanchezza da notifica inondano l'utente di richieste di approvazione finché ne approva una per errore o per sfinimento. L'MFA è essenziale, e da sola non basta.

4 Attacchi di rete

Gli attacchi a livello di rete prendono di mira l'infrastruttura attraverso cui viaggiano i dati, più che le applicazioni o gli utenti alle due estremità.

4.1 Man-in-the-Middle (MitM)

Un attacco MitM mette l'attaccante tra due parti che comunicano, così che possa intercettare, leggere e magari modificare il traffico senza che nessuna se ne accorga. Diverse tecniche permettono questa posizione:

- **ARP poisoning**: abusa del protocollo ARP, che associa indirizzi IP e indirizzi MAC in una rete locale. Con risposte ARP falsificate l'attaccante fa associare agli altri host il proprio MAC a un IP legittimo, instradando il traffico attraverso la sua macchina.
- **DNS spoofing**: corrompe le voci della cache DNS per reindirizzare le risoluzioni verso indirizzi controllati dall'attaccante: chi digita «banca.it» finisce sul server dell'attaccante.
- **SSL stripping**: declassa HTTPS a HTTP. L'attaccante intercetta il reindirizzamento da HTTP a HTTPS e mantiene una connessione HTTP con l'utente mentre fa da proxy HTTPS verso il server reale. La difesa principale è HSTS (HTTP Strict Transport Security).

4.2 Denial of Service (DoS) e Distributed DoS (DDoS)

Un attacco DoS sommerge un sistema di traffico o richieste finché non riesce più a servire gli utenti legittimi. Il DDoS lo distribuisce su migliaia o milioni di macchine compromesse (una botnet), quindi non si ferma filtrando un singolo IP di origine. I DDoS moderni agiscono su più livelli:

Tabella 1

Tipo	Livello	Meccanismo	Esempi
Volumetrico	Rete (L3/L4)	Satura la banda con traffico grezzo	UDP flood, ICMP flood, amplificazione DNS
Di protocollo	Trasporto (L4)	Esaurisce le tabelle di stato delle connessioni del server	SYN flood, Ping of Death, Smurf
Applicativo	Applicazione (L7)	Esaurisce le risorse dell'applicazione con richieste dall'aspetto legittimo	HTTP flood, Slowloris, ReDoS

Gli **attacchi di amplificazione** meritano una menzione. Falsificando l'IP di origine di una piccola richiesta verso un servizio che restituisce una risposta molto più grande (DNS, NTP, memcached), un attaccante può dirigere volumi enormi di traffico verso un bersaglio con pochissima banda in uscita. L'attacco del 2018 contro GitHub ha raggiunto 1,35 Tbps tramite amplificazione memcached, il più grande mai registrato fino ad allora.

4.3 Port scanning ed enumerazione

Prima di attaccare un sistema, l'attaccante deve sapere cosa ci gira. Gli scanner di porte, **Nmap** su tutti, inviano sonde a un intervallo di porte e analizzano le risposte per capire quali sono aperte, quali servizi ascoltano e quali versioni di software girano. È una sonda attiva, ma così routinaria che su un host esposto a internet si perde nel rumore di fondo delle scansioni continue, e ciò che rivela decide direttamente quali exploit tentare.

5 Attacchi alle applicazioni web

Le applicazioni web sono tra le superfici più bersagliate: pubbliche, spesso complesse e di frequente con difetti introdotti in fase di sviluppo. La **OWASP Top 10** è il riferimento standard di settore per i loro rischi. Questi sono i più significativi dal punto di vista tecnico.

5.1 SQL injection (SQLi)

La SQL injection si verifica quando l'input dell'utente finisce in una query al database senza il giusto trattamento, permettendo all'attaccante di cambiare la logica della query. Prendi un form di login che costruisce questa query:

```sql
SELECT * FROM users WHERE username = '[input]' AND password = '[input]'
```

Se l'attaccante inserisce `' OR '1'='1` come nome utente, la query diventa:

```sql
SELECT * FROM users WHERE username = '' OR '1'='1' AND password = ''
```

Poiché `'1'='1'` è sempre vera, la query restituisce degli utenti e l'autenticazione è aggirata. Una SQLi più sofisticata può estrarre un intero database, scrivere file sul server o, in certe configurazioni, eseguire comandi del sistema operativo. Le varianti includono la **blind SQLi** (nessun output diretto: l'attaccante deduce informazioni dal comportamento o dai tempi dell'applicazione), la **time-based blind SQLi** (ritardi deliberati come segnale binario) e la **out-of-band SQLi** (dati esfiltrati tramite richieste DNS o HTTP innescate dal server del database). La difesa è la stessa per tutte: query parametrizzate, mai concatenazione di stringhe.

5.2 Cross-Site Scripting (XSS)

L'XSS si verifica quando un attaccante inietta script malevoli in pagine viste da altri utenti. Il browser tratta lo script iniettato come legittimo e gli dà accesso a tutto ciò che possono raggiungere gli script legittimi: cookie, token di sessione, local storage, DOM e la possibilità di fare richieste autenticate per conto dell'utente.

L'**XSS riflesso** arriva tramite un URL costruito ad arte: lo script è nella richiesta e viene riflesso nella risposta, quindi la vittima deve cliccare il link. L'**XSS memorizzato** (persistente) viene iniettato nell'archivio dell'applicazione (un commento, il nome di un profilo, un post su un forum) e gira per chiunque veda quel contenuto, il che lo rende molto più pericoloso, perché non richiede una consegna mirata. L'**XSS basato sul DOM** avviene interamente nel browser, quando il JavaScript lato client elabora in modo non sicuro dati controllati dall'attaccante.

5.3 Cross-Site Request Forgery (CSRF)

Il CSRF sfrutta il fatto che i browser allegano automaticamente le credenziali (cookie) alle richieste verso un sito, da qualunque origine provengano. Se un attaccante induce un utente loggato a caricare una pagina che controlla, quella pagina può fare in silenzio richieste autenticate al sito bersaglio (inviare form, cambiare impostazioni, avviare trasferimenti) a nome della vittima.

La difesa classica è un token CSRF: un valore segreto e imprevedibile incluso nei form e validato dal server. Un attaccante di un'altra origine non può leggerlo per via della Same-Origin Policy, quindi non può inserirlo nelle richieste falsificate. Le difese moderne comprendono anche i cookie `SameSite`.

5.4 Server-Side Request Forgery (SSRF)

L'SSRF è tra le vulnerabilità web moderne più pericolose. Si verifica quando un'applicazione recupera una risorsa remota in base a un input fornito dall'utente senza una validazione adeguata. L'attaccante può fornire un URL interno, come `http://169.254.169.254/latest/meta-data/` su AWS, e far interrogare al server servizi interni non raggiungibili da internet. Negli ambienti cloud, un'SSRF contro il servizio di metadati dell'istanza può fornire credenziali temporanee con permessi IAM rilevanti.

> **CASO DI STUDIO: CAPITAL ONE (2019), SSRF NEL CLOUD**
>
> A marzo 2019 un ex dipendente di AWS sfruttò un web application firewall configurato male su un'istanza EC2 di Capital One. Il firewall poteva essere indotto a fare richieste lato server, e l'attaccante le usò per interrogare il servizio di metadati dell'istanza e ottenere credenziali AWS temporanee legate a un ruolo IAM troppo permissivo. Con quelle elencò e scaricò bucket S3 contenenti i dati di circa 100 milioni di persone negli Stati Uniti e 6 milioni in Canada, tra cui nomi, indirizzi e informazioni legate al credito, e circa 140.000 numeri di previdenza sociale. L'attaccante fu identificato perché si vantò online. Il difetto tecnico fu la combinazione di un firewall soggetto a SSRF e di un ruolo IAM con permessi S3 eccessivi: il principio del minimo privilegio, dare ai servizi solo ciò che serve, avrebbe limitato molto i danni.

5.5 Deserializzazione non sicura

La serializzazione converte un oggetto in un formato che si può salvare o trasmettere (JSON, XML, binario); la deserializzazione ricostruisce l'oggetto. Se un'applicazione deserializza dati forniti dall'utente senza validarli, un attaccante può costruire un oggetto serializzato malevolo che, deserializzato, esegue codice arbitrario sul server. Le falle di deserializzazione in Java sono state particolarmente gravi: la gadget chain di Apache Commons Collections, resa pubblica nel 2015, permetteva l'esecuzione di codice remoto contro qualsiasi applicazione Java che usasse quella libreria, compresi prodotti enterprise come WebLogic, WebSphere e Jenkins.

6 Malware

Il software malevolo è lo strumento principale con cui gli attaccanti stabiliscono e mantengono l'accesso ai sistemi compromessi. Conoscere le categorie principali aiuta a capire quali difese servono e perché la sicurezza degli endpoint è così difficile.

6.1 Virus e worm

Un **virus** si attacca a un programma legittimo e ha bisogno di un'azione umana per diffondersi (aprire un file infetto, eseguire un eseguibile infetto). Un **worm** si diffonde da solo attraverso le reti sfruttando vulnerabilità. WannaCry, che nel 2017 ha infettato più di 200.000 sistemi in circa 150 paesi, era un worm che usava l'exploit EternalBlue (sviluppato dalla NSA e fatto trapelare dagli Shadow Brokers) per diffondersi attraverso servizi SMB non aggiornati.

6.2 Trojan

Un Trojan si maschera da software legittimo mentre compie in background funzioni malevole. A differenza dei virus, i Trojan non si replicano: contano sull'ingegneria sociale per farsi installare (un download di software craccato, una finta utility di sistema, un allegato malevolo). Una volta dentro, un Trojan può installare una backdoor, rubare credenziali, unirsi a una botnet o scaricare altri payload.

6.3 Ransomware

Il ransomware cifra i file della vittima e chiede un pagamento per la chiave. È passato da fastidio per i privati all'inizio degli anni 2010 a una delle principali minacce per aziende, ospedali, governi e infrastrutture critiche.

Le operazioni moderne di **ransomware-as-a-service (RaaS)**, come LockBit e BlackCat/ALPHV, funzionano come imprese di software: un gruppo centrale sviluppa e mantiene il ransomware e l'infrastruttura di negoziazione, mentre gli affiliati conducono le intrusioni e versano al gruppo centrale una quota dei riscatti. Questa divisione del lavoro ha moltiplicato numero e sofisticazione degli attacchi (anche se le forze dell'ordine hanno poi colpito alcuni di questi gruppi, altri ne prendono il posto).

Gli attacchi odierni usano tipicamente la **doppia estorsione**: oltre a cifrare i file, l'attaccante esfiltra prima i dati e minaccia di pubblicarli se il riscatto non viene pagato. Questo elimina la vecchia difesa del «abbiamo i backup, non paghiamo».

> **CASO DI STUDIO: COLONIAL PIPELINE (2021)**
>
> A maggio 2021 il gruppo DarkSide attaccò Colonial Pipeline, gestore del più grande oleodotto di carburanti degli Stati Uniti. L'accesso iniziale fu un account VPN compromesso: la password di un profilo legacy non più in uso ma non disattivato, e soprattutto senza autenticazione a più fattori. Colonial fermò le operazioni in via precauzionale, causando carenze di carburante sulla costa orientale e un breve rialzo dei prezzi. L'azienda pagò circa 4,4 milioni di dollari di riscatto, e l'FBI ne recuperò poi circa 2,3 milioni. L'attacco mostrò che il ransomware contro le infrastrutture critiche non era un'ipotesi, e che l'esposizione va oltre i sistemi operativi fino all'IT che li sostiene.

6.4 Rootkit

Un rootkit è un malware progettato per nascondere la propria presenza e quella di altro malware. I rootkit a livello kernel agganciano le chiamate di sistema per nascondere file, processi e connessioni di rete al sistema operativo e agli strumenti che ci girano sopra. Un sistema con un rootkit nel kernel non può essere considerato affidabile nel riportare il proprio stato, perché il rootkit intercetta le stesse chiamate che gli strumenti di sicurezza usano per ispezionarlo.

6.5 Spyware e keylogger

Lo spyware monitora in silenzio l'attività dell'utente e invia i dati all'attaccante: cronologia di navigazione, tasti premuti, schermate, microfono e fotocamera, contenuto degli appunti. I **keylogger** registrano in particolare i tasti premuti, catturando password, numeri di carta e qualunque altro

testo digitato. All'estremo più sofisticato ci sono prodotti commerciali come Pegasus, sviluppato da NSO Group e venduto a clienti governativi, che sfruttano vulnerabilità zero-day per prendere il controllo di un dispositivo senza alcuna interazione dell'utente.

6.6 Botnet

Una botnet è una rete di macchine compromesse (bot o zombie) controllate dall'attaccante tramite infrastruttura C2, usata per DDoS, spam, credential stuffing, mining di criptovalute e distribuzione di altro malware. La botnet Mirai, che nel 2016 lanciò un DDoS da oltre un terabit al secondo contro il fornitore DNS Dyn e fece cadere servizi come Twitter, Reddit e Netflix, era composta in prevalenza da dispositivi IoT (telecamere, router, videoregistratori) le cui credenziali predefinite non erano mai state cambiate.

7 Advanced Persistent Threat (APT)

Le APT sono attacchi sofisticati e di lunga durata, tipicamente condotti da attori statali o da gruppi criminali molto organizzati con risorse significative. Le caratterizzano la persistenza (accesso mantenuto per mesi o anni), la furtività (evitare di essere scoperti mentre si perseguono gli obiettivi) e la mira (puntare a bersagli specifici di alto valore invece di compromettere qualunque sistema disponibile).

7.1 Attacchi alla supply chain

Invece di attaccare direttamente un bersaglio ben difeso, un attacco alla supply chain compromette una terza parte fidata (un fornitore di software, un fornitore di servizi gestiti, un produttore hardware) e usa quel rapporto come via d'ingresso.

> **CASO DI STUDIO: SOLARWINDS / SUNBURST (2020)**
>
> A dicembre 2020 FireEye rivelò che alcuni attaccanti avevano compromesso la pipeline di build di SolarWinds, fornitore di software di gestione IT, inserendo codice malevolo, chiamato SUNBURST, in un aggiornamento firmato della piattaforma Orion. L'aggiornamento raggiunse circa 18.000 clienti di SolarWinds, tra cui dipartimenti del governo statunitense (Tesoro, Commercio, Sicurezza Interna, Stato) e grandi aziende tecnologiche. SUNBURST era estremamente accurato: restava dormiente fino a due settimane dopo l'installazione per eludere l'analisi in sandbox, comunicava tramite traffico DNS dall'aspetto legittimo, imitava il normale traffico di Orion e cercava strumenti di sicurezza per adattare il proprio comportamento. Il governo statunitense attribuì l'operazione all'intelligence estera russa (il gruppo APT29). La lezione: anche organizzazioni con programmi di sicurezza maturi possono essere compromesse tramite aggiornamenti fidati, e difendersi dagli attacchi alla supply chain richiede un modo di pensare diverso dalla difesa del perimetro.

7.2 Exploit zero-day

Uno zero-day è una vulnerabilità sconosciuta al produttore, per cui non esiste alcuna patch: il produttore ha avuto «zero giorni» per correggerla. Zero-day affidabili in software molto diffuso sono tra i beni più preziosi dell'ecosistema offensivo, e governi e agenzie di intelligence li pagano milioni. Il worm Stuxnet, scoperto nel 2010 e ampiamente attribuito a un'operazione congiunta di Stati Uniti e Israele (mai confermata ufficialmente da nessuno dei due governi), usò più vulnerabilità zero-day

contemporaneamente, un numero senza precedenti, per compromettere gli impianti iraniani di arricchimento dell'uranio e danneggiare fisicamente le centrifughe manipolandone i sistemi di controllo mentre riportava agli operatori un funzionamento normale.

8 Sfruttamento di vulnerabilità note

Oltre agli zero-day, gli attaccanti sfruttano di routine vulnerabilità note per cui esistono patch non ancora applicate. Il divario tra la divulgazione e l'applicazione diffusa delle patch è una superficie d'attacco primaria per attaccanti sia opportunisti sia mirati.

Tabella 2

Classe	Meccanismo	Impatto tipico
Buffer overflow	Scrivere dati oltre i limiti di un buffer allocato, sovrascrivendo la memoria adiacente, compresi gli indirizzi di ritorno	Esecuzione di codice arbitrario, escalation dei privilegi
Use-after-free	Accedere alla memoria dopo che è stata liberata e magari riassegnata a un altro oggetto	Esecuzione di codice arbitrario, divulgazione di informazioni
Integer overflow	Un'operazione aritmetica produce un valore troppo grande per il tipo e si riavvolge su uno inatteso	Buffer overflow, errori logici, aggiramenti della sicurezza
Path traversal	Usare sequenze `../` per uscire dalla directory prevista e raggiungere file arbitrari	Accesso non autorizzato ai file, furto di credenziali
Command injection	Input dell'utente inserito senza controllo in comandi del sistema operativo eseguiti dall'applicazione	Esecuzione di codice remoto con i privilegi dell'applicazione
XML External Entity (XXE)	Un parser XML elabora riferimenti a entità esterne in un XML fornito dall'attaccante	Lettura di file, SSRF, denial of service

9 Minacce interne

Non tutte le minacce vengono da fuori. Le minacce interne sono azioni dolose o negligenti di dipendenti, collaboratori o altre persone fidate con accesso legittimo, e sono una categoria significativa e spesso sottovalutata.

Gli **insider malevoli** abusano deliberatamente del proprio accesso, per profitto personale, vendetta o ideologia. L'esfiltrazione di documenti NSA da parte di Edward Snowden è il caso più famoso su larga scala, ma la maggior parte degli incidenti di insider malevoli riguarda furti di dati per vantaggio competitivo, frodi finanziarie o sabotaggio. Gli **insider negligenti** causano danni per disattenzione: cliccare link di phishing, configurare male lo storage cloud, perdere dispositivi non cifrati, condividere credenziali, saltare le procedure. Circa due terzi delle violazioni nel Data Breach Investigations Report di Verizon coinvolgono un elemento umano.

> **L'EPIDEMIA DELLE CONFIGURAZIONI SBAGLIATE**

> Lo storage cloud configurato male è dietro un numero enorme di esposizioni di dati: bucket S3 accessibili pubblicamente, indici Elasticsearch esposti, database Firebase leggibili da chiunque. Non sono attacchi sofisticati. Sono scansioni automatiche di schemi noti di configurazione errata seguite da uno sfruttamento banale, e il rapporto di Verizon elenca regolarmente la configurazione errata tra i principali errori all'origine delle violazioni.

10 Attacchi crittografici

La crittografia è il fondamento matematico della maggior parte dei sistemi di sicurezza. Gli attacchi contro di essa prendono di mira gli algoritmi, le loro implementazioni o i protocolli che li usano.

10.1 Attacchi di downgrade

Un attacco di downgrade costringe una connessione a usare una versione di protocollo o una suite di cifratura più vecchia e debole, che l'attaccante può poi attaccare. POODLE (2014) sfruttò la possibilità di riportare le connessioni a SSL 3.0, che aveva debolezze sfruttabili. Altri noti attacchi a TLS funzionano diversamente: BEAST colpiva una debolezza della modalità CBC nelle vecchie versioni di TLS, mentre CRIME e BREACH sfruttavano le informazioni che trapelano dalla compressione.

10.2 Collisioni di hash

Le funzioni hash crittografiche devono resistere alle collisioni: dovrebbe essere computazionalmente impraticabile trovare due input diversi con lo stesso hash. Quando questo vale meno, firme digitali e validazione dei certificati possono essere falsificate. MD5 è rotto nella pratica dal 2004, e SHA-1 è caduto con l'attacco SHAttered di Google nel 2017, che ha prodotto due file PDF diversi con lo stesso hash SHA-1.

10.3 Forza bruta e rainbow table

Gli hash delle password salvati in un database possono essere attaccati offline: con il file degli hash, un attaccante può provare a recuperare le password senza toccare il sistema in produzione. Un attacco a forza bruta prova ogni combinazione, uno a dizionario prova password comuni e loro varianti, e uno con rainbow table usa catene di hash precalcolate per recuperare le password rapidamente, scambiando spazio di archiviazione con tempo di calcolo.

Il **salting**, aggiungere un valore casuale univoco a ogni password prima dell'hash, sconfigge le rainbow table rendendo impraticabile il precalcolo. Le moderne funzioni di hashing per password come bcrypt, scrypt e Argon2 sono volutamente costose da calcolare, così la forza bruta resta lenta anche su hardware potente.

11 Il modello di difesa: pensare a strati

Una difesa efficace non è mai un singolo controllo. È un'architettura a strati, la difesa in profondità, in cui più controlli indipendenti devono essere tutti aggirati perché l'attaccante riesca, e il cedimento di uno strato non significa compromissione totale.

Tabella 3

Strato	Controlli	Cosa affronta
Perimetro	Firewall, WAF, mitigazione DDoS, segmentazione di rete	Riduce la superficie d'attacco e blocca il traffico noto come malevolo
Identità	MFA, gestione degli accessi privilegiati, architettura zero trust	Rende meno utili le credenziali rubate e limita il movimento laterale
Endpoint	EDR/XDR, allowlisting delle applicazioni, gestione delle patch	Rileva e contiene il malware e riduce l'esposizione alle vulnerabilità
Applicazione	SDLC sicuro, SAST/DAST, scansione delle dipendenze, gestione dei segreti	Previene vulnerabilità nel codice e nelle dipendenze
Dati	Cifratura a riposo e in transito, DLP, controlli d'accesso, backup	Limita l'impatto di una violazione riuscita e rende possibile il ripristino
Rilevamento	SIEM, aggregazione dei log, threat hunting, rilevamento di anomalie	Individua gli attacchi in corso e riduce il dwell time
Risposta	Piano di risposta agli incidenti, capacità forense, comunicazione di crisi	Contiene e recupera dagli attacchi riusciti

I CONTROLLI PIÙ EFFICACI

Con un budget di sicurezza limitato, tre controlli danno un valore sproporzionato. (1) **Autenticazione a più fattori** su tutti gli account, soprattutto quelli privilegiati: ferma la maggior parte degli attacchi automatici alle credenziali (meglio se con metodi resistenti al phishing come le chiavi FIDO2, vista l'AiTM). (2) **Gestione delle patch**: gran parte delle vulnerabilità sfruttate è nota e già correggibile quando avviene l'attacco. (3) **Backup regolari, testati e offline**: l'unica difesa affidabile contro il ransomware che non passi dal pagare.

12 Conclusione

Il panorama delle minacce descritto qui non è statico. Emergono continuamente nuove tecniche, quelle esistenti vengono affinate e automatizzate, e la superficie d'attacco cresce con ogni nuovo servizio, ogni nuova integrazione e ogni nuovo dipendente.

Ma i fondamenti della difesa sono più stabili dei dettagli dei singoli attacchi. Capire come funzionano gli attacchi, in modo meccanico e non solo per categorie, è il presupposto per difese che tengono. Un attaccante che ha passato mesi a studiare il tuo ambiente, i tuoi sistemi e le tue persone non verrà fermato da una casella di conformità spuntata. Lo fermeranno controlli a strati, rilevamento attivo e una risposta allenata.

La sicurezza non è un prodotto che si compra; è una disciplina continua di comprensione, investimento e miglioramento. In un mondo in cui gli attaccanti ottimizzano per la strada di minor resistenza, essere un bersaglio sensibilmente più difficile spesso significa essere quello che si lasciano alle spalle.

Questo articolo riflette lo stato del panorama delle minacce a inizio 2026. Vulnerabilità, strumenti e tecniche evolvono in fretta. Per indicazioni operative consulta gli avvisi aggiornati di CISA, NIST e degli ISAC di settore, oppure del tuo CSIRT nazionale.

COME CITARE QUESTO ARTICOLO

Francesco Barbato (2026). Gli attacchi informatici spiegati: guida tecnica a come lavorano davvero gli attaccanti. localhost:3000.

Versione online: http://localhost:3000/it/blog/attacchi-informatici-guida-tecnica