Isabelle Adjetey– Cybersecurity Analyst

Panorama degli Attacchi Informatici: Remediation & Prevenzione

Agosto 2025

Questo playbook nasce dalla mia esigenza di avere, in un unico strumento, un quadro sintetico ma completo delle principali minacce informatiche e delle misure di contenimento e prevenzione. Serve tanto come prontuario di rapida consultazione durante esercitazioni hands-on quanto come base per lo studio e l'allineamento di conoscenze.

1. Malware

T1587.001 https://attack.mitre.org/techniques/T1587/001/

1.1 Descrizione

Software creato per infiltrarsi in un sistema e compiere azioni dannose senza il consenso dell'utente. Categorie principali:

- **Virus**
- **Worm**
- **Trojan**

Isabelle Adjetey– Cybersecurity Analyst

Ransomware

Spyware/Adware

Rootkit

1.2 Vettori di Attacco e Indicatori di Compromissione (IoC)

Vettori comuni**

- Download da siti compromessi e drive-by download
- Allegati email (doc, pdf, zip) con macro o eseguibili
- Vulnerabilità non patchate in software desktop e server

IoC tipici

- ❖ Processi sconosciuti in esecuzione (es. “svch0st.exe” al posto di “svchost.exe”)
- ❖ Picchi di utilizzo CPU o disco senza motivo
- ❖ Connessioni outbound verso server C2 su porte non standard

1.3 Remediation

- Contenimento
  - Disconnettere l’host dalla rete di laboratorio (quarantena VLAN)
  - Bloccare account utente compromessi
- Investigazione Forense
  - Dump di memoria e acquisizione volumi con tool EDR/XDR
  - Raccolta di log di sistema, event log Windows e audit Linux
- Eliminazione
  - Scansione full-disk in modalità offline con antivirus enterprise
  - Rimozione manuale di chiavi di autostart (Registro di sistema, cron job)
- Ripristino
  - Reinstallazione da immagine master “clean” o ripristino backup verificati
  - Verifica dell’integrità delle copie di backup

1.4 Prevenzione

- Configurare una Endpoint Protection Platform (EPP) con behavior-blocking
- Implementare Application Whitelisting (es. Windows AppLocker)
- Automatizzare il patch management con tool centralizzati
- Creare esercitazioni di riconoscimento di allegati malevoli su macchine virtuali

2. Phishing, Spear Phishing, Smishing & Vishing

T1566 https://attack.mitre.org/techniques/T1566/

2.1 Descrizione

Tecniche di ingegneria sociale mirate a carpire credenziali, diffondere malware o ottenere informazioni riservate.

2.2 Vettori di Attacco e IoC

- Email con link che conducano a pagine di login fasulle
- SMS con URL abbreviati
- Chiamate vocali che si spacciano per IT o istituti finanziari

Indicatori

- ❖ Domini simili (typo-squatting)
- ❖ Mittenti esterni non definiti nei record DNS aziendali
- ❖ Richieste urgenti di modifica password

2.3 Remediation

- Segnalazione
  - Inoltrare al SOC e marcare come “phishing” nel gateway email/SMS
  - Rimuovere tutti i link e bloccare l’apertura degli allegati
- Contenimento
  - Reset password e invalidazione token di sessione
- Investigazione
  - Analisi dei log di autenticazione (VPN, SSO, Active Directory)
  - Verifica accessi da IP sconosciuti
- Pulizia Endpoint
  - Scansione antivirus/antimalware
  - Rimozione payload eventualmente scaricati

2.4 Prevenzione

- MFA obbligatoria su tutti i servizi critici
- Gateway antiphishing con sandboxing dinamico
- Phish-testing periodico con survey e feedback individuale
- Implementazione di DMARC, DKIM e SPF

3. Denial of Service (DoS / DDoS)

T1498 https://attack.mitre.org/techniques/T1498/

3.1 Descrizione

Attacco volto a rendere indisponibile un servizio sovraccaricando risorse di rete o server.

3.2 Vettori di Attacco e IoC

- Botnet distribuite
- Reflection / amplification (DNS, NTP, Memcached)

Indicatori

❖ Picchi anomali di traffico in ingresso (Gbps/Tbps)
❖ High rate di SYN incomplete o pacchetti UDP amplificati
❖ Errori di timeout sui firewall

3.3 Remediation

3.1. Mitigazione Temporanea

- Attivare scrubbing center del provider
- Blackholing IP aggressivi

3.2. Bilanciamento del Carico

- Distribuire traffico su più data center/regioni
- Rate-limiting su endpoint critici

3.3. Ripristino

- Verifica integrità database dopo stress
- Test end-to-end dei servizi

3.4 Prevenzione

- CDN e WAF con regole anti-DDoS
- Circuit breaker e threshold di rate limiting
- Stress test annuali di resilienza
- Contratti con vendor specializzati (Cloudflare, AWS Shield)

4.Man-in-the-Middle (MITM)

T1557 https://attack.mitre.org/techniques/T1557/

4.1 Descrizione

Intercettazione e possibile alterazione del flusso di comunicazioni tra due endpoint.

4.2 Vettori di Attacco e IoC

- Wi-Fi pubblici non protetti
- ARP/DNS spoofing
- SSL stripping

Indicatori

- ❖ Certificati TLS non validi
- ❖ Modifiche DNS sospette
- ❖ Pacchetti duplicati in capture

4.3 Remediation

- Revoca Certificati
  - Revocare e riemettere TLS compromessi
- Logout Forzato
  - Reset token e sessioni
- Packet Capture
  - Analisi con Wireshark per identificare attaccante
- Patch e Hardening
  - Firmware update su switch/router
  - Abilitare Dynamic ARP Inspection e DNSSEC

4.4 Prevenzione

- HTTPS + HSTS obbligatori
- VPN aziendale con mutual authentication
- Anti-spoofing a livello L2/L3
- Monitoraggio DNS e alert su anomalie

5. Web Application Attacks (SQLi, XSS, CSRF)

T1190 https://attack.mitre.org/techniques/T1190/

T1189 https://attack.mitre.org/techniques/T1189/

CAPEC-62 https://capec.mitre.org/data/definitions/62.html

5.1 Descrizione

Sfruttamento di input non sanificati o di trust in sessioni per eseguire codice malevolo o manipolare dati.

5.2 Vettori di Attacco e IoC

- Parametri GET/POST non sanitizzati
- Cookie senza HttpOnly/Secure

- Token CSRF statici

Indicatori

- ❖ Pattern di attacco nei log (es. `' OR '1'='1`)
- ❖ Script inline non autorizzati
- ❖ POST automatici da domini esterni

5.3 Remediation

- Disabilitare Funzionalità
  - Rimuovere feature beta non in uso
- Sanitizzazione Input
  - Prepared statements/ORM
  - Escape output HTML
- Token Security
  - Rigenerare token CSRF ad ogni richiesta
- Analisi WAF
  - Aggiornare signature OWASP Top 10

5.4 Prevenzione

- Framework con escaping automatico (React, Django)
- Content Security Policy restrittiva
- Flag HttpOnly e Secure sui cookie
- Code review e pen test trimestrali

6. Zero-Day Exploit

T1203 https://attack.mitre.org/techniques/T1203/

6.1 Descrizione

Sfruttamento di vulnerabilità sconosciute al vendor, prive di patch ufficiali.

6.2 Vettori di Attacco e IoC

- Documenti Office con macro malevole
- Exploit kit personalizzati

Indicatori

- ❖ Crash applicazioni aggiornate
- ❖ Download di payload da URL brevi

❖ Alert EDR su comportamenti anomali

6.3 Remediation

- Contenimento
  - Isolare endpoint compromessi
- Regole Comportamentali**
  - Deploy di policy EDR basate su comportamento
- Threat Intel
  - Condivisione IoC (MISP, CERT)
- Patch di Emergenza
- Applicazione workaround in attesa del fix

6.4 Prevenzione

- Feed di threat intelligence zero-day
- Subnet separate per ambienti sensibili
- Sandboxing documenti sospetti
- Vulnerability management continuo

7. Supply Chain Attack

T1195 https://attack.mitre.org/techniques/T1195/

7.1 Descrizione

Compromissione di fornitori o componenti terzi per introdurre malware direttamente nel target.

7.2 Vettori di Attacco e IoC

- Aggiornamenti software alterati
- Librerie infette su repository pubblici

Indicatori

❖ Hash dei pacchetti non corrispondente
❖ Modifiche non firmate nella pipeline
❖ Script sconosciuti in provisioning

7.3 Remediation

- Revoca & Restore
  - Revocare certificati e ripristinare snapshot sicuri

- Software Composition Analysis
  - Scansione dipendenze con SCA tool (Snyk, Nexus)
- Audit Pipeline
  - Verifica firme digitali e checksum
- Comunicazione Fornitori
  - Richiedere report forense e patch ufficiali

7.4 Prevenzione

- Framework secure supply chain (Sigstore, in-toto)
- Policy di code signing e verifica metadati
- Pen test su componenti terzi
- Continuous dependency mapping

8. Cloud Misconfiguration

T1530 https://attack.mitre.org/techniques/T1530/

8.1 Descrizione

Errori di configurazione di risorse cloud (storage, compute, IAM) che espongono dati o servizi.

8.2 Vettori di Attacco e IoC

- Bucket S3 pubblici non intenzionali
- Security group aperti a 0.0.0.0/0
- Ruoli IAM troppo permissivi

Indicatori

- ❖ Accessi anonimi a storage
- ❖ Modifiche security group senza change request
- ❖ Eventi console cloud anomali

8.3 Remediation

- Chiusura & Revoca
  - Disabilitare risorse esposte
  - Revocare permessi eccessivi
- Ripristino da Snapshot
  - Ripristinare bucket/istanze puliti
- Verifica Forense
  - Analisi log CloudTrail/Activity Log

- Hardening Automatizzato
    - IaC con rollback di drift

8.4 Prevenzione

- IaC (Terraform, CloudFormation) con policy di validazione
- CSPM per monitoraggio continuo
- Principle of least privilege IAM
- Scan giornaliero delle configurazioni

9. Attacchi su Dispositivi IoT

T0814 https://attack.mitre.org/techniques/T0814/

9.1 Descrizione

Dispositivi con firmware obsoleto o credenziali di default usati come pivot o botnet.

9.2 Vettori di Attacco e IoC

- Telnet/SSH aperti con password factory
- Backdoor integrate in firmware

Indicatori

- ❖ Login con credenziali di fabbrica
- ❖ Traffico verso server C2 esterni
- ❖ Richieste firmware non autorizzate

9.3 Remediation

- Isolamento VLAN
    - Spostare device compromessi in subnet dedicate
- Firmware Recovery
    - Flash firmware ufficiale verificato
- Scansione Rete
    - Discovery per individuare altri device vulnerabili
- Analisi Traffic
    - Raccogliere netflow e individuare anomalie

9.4 Prevenzione

- Cambiare credenziali di default e applicare password policy
- Segmentare device IoT in rete dedicata con NAC
- Aggiornamenti OTA programmati e firmati
- Test di sicurezza firmware pre-produzione

10 Glossario

ACL: Access Control List

ARP: Address Resolution Protocol

C2: Command and Control

CDN: Content Delivery Network

CSPM: Cloud Security Posture Management

CSRF: Cross-Site Request Forgery

DNS: Domain Name System

DNSSEC: Domain Name System Security Extensions

DoS/DDoS: Denial of Service / Distributed Denial of Service

EDR/XDR: Endpoint Detection & Response / Extended Detection & Response

EPP: Endpoint Protection Platform

FTP: File Transfer Protocol

HSTS: HTTP Strict Transport Security

HTTP: Hypertext Transfer Protocol

HTTPS: Hypertext Transfer Protocol Secure

ICMP: Internet Control Message Protocol

IaC: Infrastructure as Code

IoC: Indicatori di Compromissione

MFA: Multi-Factor Authentication

MITM: Man-in-the-Middle

NAC: Network Access Control

NAT: Network Address Translation

ORM: Object-Relational Mapping

OTA: Over The Air

PCAP: Packet Capture

SCA: Software Composition Analysis

SQLi: SQL Injection

SSH: Secure Shell

TCP: Transmission Control Protocol

TLS: Transport Layer Security

UDP: User Datagram Protocol

URL: Uniform Resource Locator

VPN: Virtual Private Network

WAF: Web Application Firewall

XSS: Cross-Site Scripting