Sicurezza Informatica e Direttiva NIS 2

Minacce Cyber e Nuova Normativa Europea

Prof. Fedeli Massimo - IIS Fermi Sacconi Cpia

Ascoli Piceno

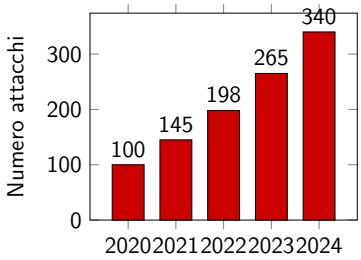
7 gennaio 2026

Indice

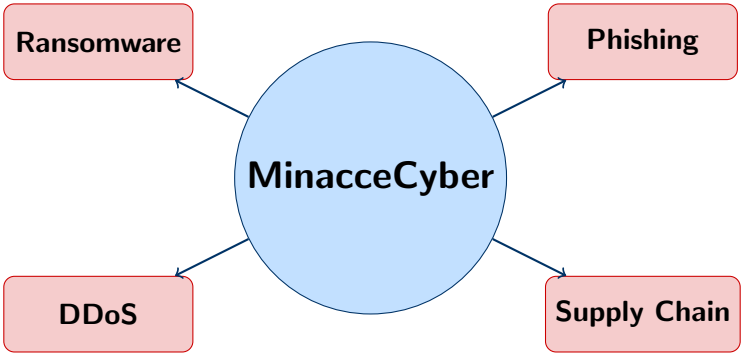
Il Panorama delle Minacce Informatiche

Scenario Attuale:

- Crescita esponenziale degli attacchi
- Maggiore complessità e sofisticazione
- Impatto su aziende, PA e infrastrutture critiche
- Evoluzione continua delle tecniche di attacco



Principali Tipologie di Attacchi



Ransomware: Il Ricatto Digitale

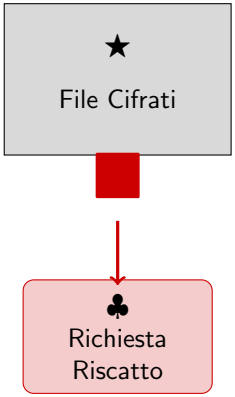
Cos'è:

- Malware che cifra i dati
- Rende inaccessibili file e sistemi
- Richiesta di riscatto in criptovaluta
- Minaccia di pubblicazione dati

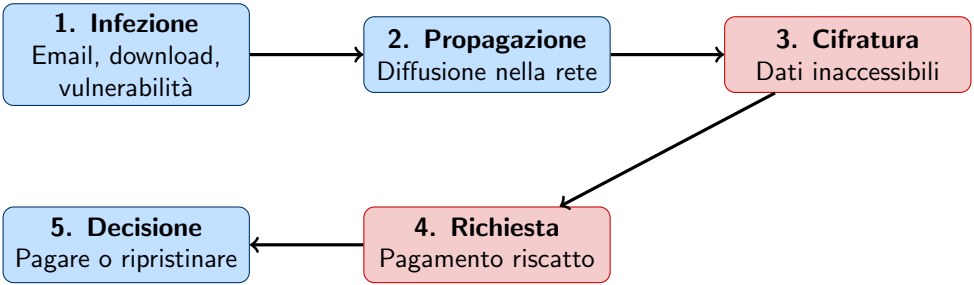
Caso emblematico:

Sistema Sanitario Irlandese (2021)

- Ospedali e ambulatori bloccati
- Sospensione servizi per giorni
- Impatto su migliaia di pazienti



Come Funziona un Attacco Ransomware



Nota Importante

Non esiste garanzia che pagando si ottengano i dati. È fondamentale avere backup offline aggiornati!

Phishing: L'Inganno via Email

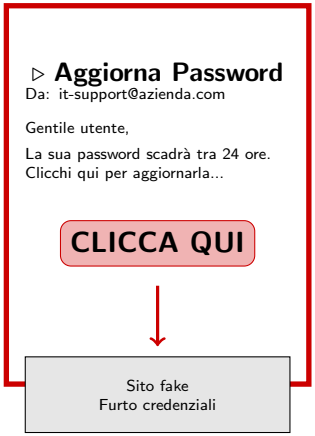
Definizione:
Email fraudolente che imitano comunicazioni ufficiali per rubare credenziali e dati sensibili.

Obiettivi:

- Password e credenziali
- Numeri carte di credito
- Dati personali sensibili
- Accesso a sistemi aziendali

Caratteristiche comuni:

- Senso di urgenza
- Mittente apparentemente legittimo
- Link a siti contraffatti



Come Riconoscere un Tentativo di Phishing

Segnali di allarme:

- Errori grammaticali o ortografici
- Indirizzo email sospetto
- Richieste urgenti
- Link con URL strani
- Allegati inaspettati
- Richieste di dati sensibili

Buone pratiche:

- ✓ Verificare sempre il mittente
- ✓ Controllare l'URL prima di cliccare
- ✓ Non fornire mai password via email
- ✓ Usare autenticazione a due fattori
- ✓ Contattare direttamente l'ente
- ✓ Segnalare email sospette

Esempio URL fraudolento

`www.banca-intesa.com` invece di `www.intesa.it`
Notare la differenza: caratteri aggiunti, domini simili ma diversi

Attacchi DDoS: Il Sovraccarico dei Sistemi

Distributed Denial of Service

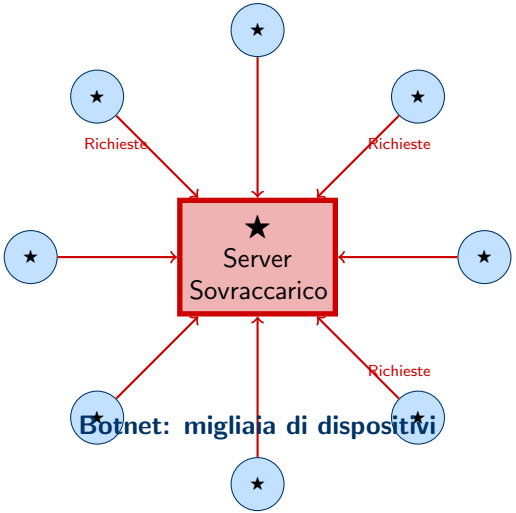
Obiettivo:
Rendere un servizio inaccessibile sovraccaricandolo con richieste massive.

Come funziona:

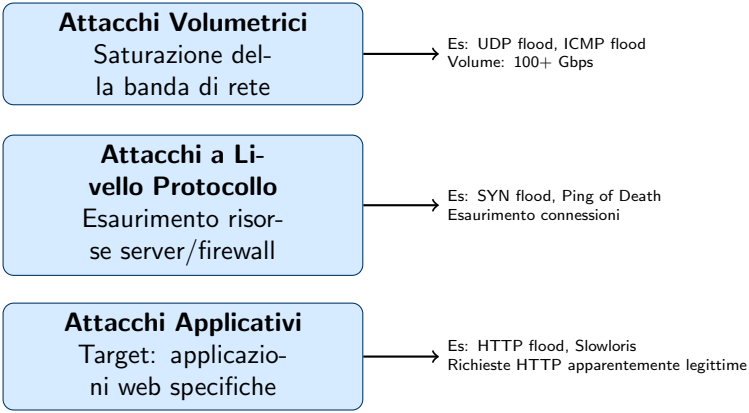
- Utilizzo di botnet (migliaia di dispositivi compromessi)
- Invio simultaneo di richieste
- Saturazione banda e risorse
- Impossibilità di servire utenti legittimi

Impatti:

- Blocco servizi online



Tipologie di Attacchi DDoS



Caso Pratico

Blocco di piattaforme bancarie online che impedisce ai clienti di accedere ai propri conti per ore o giorni, causando disservizi massivi.

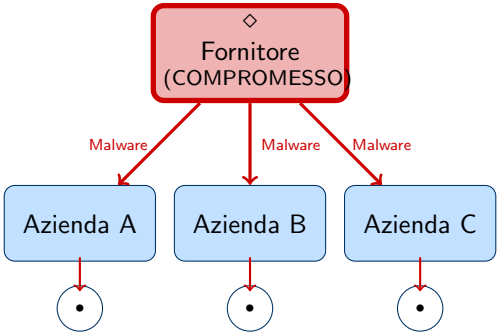
Supply Chain Attack: L'Attacco alla Catena di Fornitura

Strategia dell'attacco:

1. Target: fornitore o partner meno protetto
2. Compromissione del fornitore
3. Propagazione all'organizzazione principale
4. Infezione multipla attraverso la catena

Perché è pericoloso:

- Difficile da rilevare
- Fiducia nei fornitori
- Effetto a cascata
- Scala d'impatto enorme



Migliaia di utenti finali infettati

Caso SolarWinds (2020): Un Attacco Emblematico

Dinamica dell'attacco:

- **Target primario:** SolarWinds (software di gestione IT)
- **Metodo:** Modifica del software Orion con malware nascosto
- **Distribuzione:** Update automatici inviati ai clienti
- **Scala:** 18.000+ organizzazioni infettate

Vittime:

- Agenzie governative USA
- Dipartimento della Difesa
- Multinazionali Fortune 500
- Istituzioni finanziarie

Conseguenze:

- Accesso prolungato ai sistemi (mesi)
- Furto di dati sensibili
- Costi di remediation miliardari
- Perdita di fiducia nel software

Lezione appresa

Necessità di verificare e monitorare costantemente anche i fornitori di fiducia. La sicurezza

Il Ruolo dell'Intelligenza Artificiale negli Attacchi

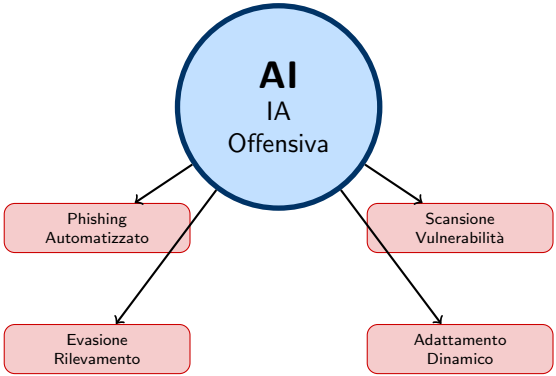
L'IA come arma degli attaccanti:

AI Applicazioni offensive:

- Phishing personalizzato e convincente
- Imitazione stile di scrittura
- Analisi vulnerabilità in tempo reale
- Identificazione target redditizi
- Evasione sistemi di rilevamento
- Botnet intelligenti e adattive

Ransomware avanzati:

- Selezione automatica vittime
- Occultamento attività malevole
- Adattamento comportamentale



Sfida crescente

La velocità e la scala degli attacchi potenziati dall'IA richiedono contromisure altrettanto avanzate

DDoS Intelligenti e IA

Botnet potenziate dall'IA:

Capacità tradizionali:

- Pattern di attacco fissi
- Rilevamento più semplice
- Comportamento prevedibile
- Difese statiche efficaci

Con IA:

- **AI** Pattern dinamici e variabili
- **AI** Elusione dei sistemi di rilevamento
- **AI** Adattamento in tempo reale
- **AI** Necessarie difese dinamiche

⊙ Vulnerabilità:
Le difese tradizionali possono identificare pattern ripetuti.

▼ Minaccia:
Difficile distinguere traffico legittimo da attacco.

Esempio concreto

Una botnet con IA può alternare tipologie di attacco (volumetrico, protocollo, applicativo) in

La Direttiva NIS 2: Risposta Europea

Direttiva (UE) 2022/2555

Data Timeline:

- Approvata: 14 dicembre 2022
- Entrata in vigore: 17 gennaio 2023
- Recepimento Stati UE: 17 ottobre 2024

Obiettivo:
Garantire un livello **elevato e omogeneo** di sicurezza informatica in tutta l'UE.

27 Stati Membri
Un unico standard di sicurezza

Principi cardine:

- Resilienza dei sistemi
- Risposta rapida agli incidenti

Perché NIS 2? I Limiti della Prima Direttiva

Direttiva NIS 1 (2016) - Problematiche riscontrate:

× Criticità:

1. **Applicazione disomogenea**
   - Discrezionalità degli Stati
   - Frammentazione normativa
   - Differenze nei livelli di sicurezza
2. **Ambito troppo ristretto**
   - Solo 4 settori coperti
   - Realtà digitali escluse
   - Copertura insufficiente
3. **Requisiti poco specifici**
   - Misure generiche
   - Mancanza di linee guida chiare
   - Implementazione incerta
4. **Monitoraggio inefficace**
   - Sistema di controllo debole
   - Sanzioni inadeguate
   - Scarsa conformità

Fattori acceleranti

Pandemia COVID-19 (lavoro remoto), **Guerra in Ucraina** (cyber warfare), **Attacchi supply chain** (interconnessione vulnerabilità)

Ampliamento dei Settori Coinvolti

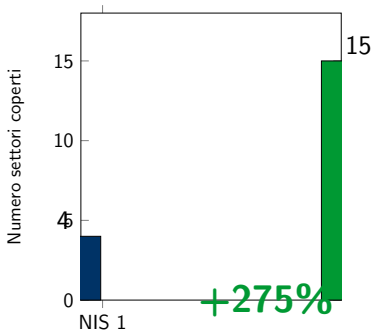
Da 4 a oltre 15 settori:

NIS 1 (2016):

- ✓ Energia
- ✓ Trasporti
- ✓ Banche
- ✓ Sanità

Nuovi settori NIS 2:

- \+ Pubblica Amministrazione
- \+ Acque reflue e rifiuti
- \+ Spazio e satelliti
- \+ Servizi postali
- \+ Produzione microchip e farmaci



Impatto

Maggiore copertura = maggiore protezione dell'ecosistema digitale europeo

Obblighi di Sicurezza Informatica

Misure concrete e documentate:

Shield Prevenzione:

- Analisi dei rischi
- Valutazione vulnerabilità
- Gestione incidenti
- Piani di continuità operativa

Protezione:

- Crittografia dati
- Controllo accessi
- Sicurezza supply chain
- Backup e ripristino

•s **Persone:**

- Formazione continua
- Consapevolezza rischi
- Responsabilità dirigenziali
- Cultura della sicurezza

Check Conformità:

- Documentazione completa
- Audit regolari
- Report periodici
- Verifiche di sicurezza

Notifica degli Incidenti e Sanzioni

Timeline di notifica:

Esempio:
Un ospedale colpito da malware deve informare immediatamente l'ACN (Agenzia per la Cybersicurezza Nazionale).

Sanzioni per inadempienza:

▼ Soggetti essenziali:
- Fino a **10 milioni €**
- Oppure **2% fatturato globale**

▼ Altri soggetti:
- Fino a **7 milioni €**
- Oppure **1,4% fatturato globale**

Responsabilità dirigenti

I dirigenti possono essere sanzionati personalmente per negligenza, con possibili interdizioni.

Applicazione in Italia

Decreto Legislativo n. 138 del 4 settembre 2024

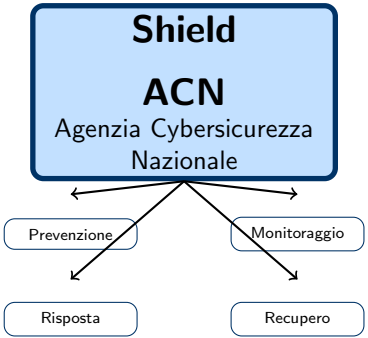
Loc Autorità competente:
Agenzia per la Cybersicurezza Nazionale (ACN)

Istituita: 2021
Dipende: Presidenza del Consiglio

Compiti principali:

onfig Strategia nazionale cybersecurity
pport Coordinamento risposta incidenti
Help Supporto tecnico PA e privati
- ▷ Gestione notifiche NIS 2

Edu Formazione e sensibilizzazione



Scadenza registrazione

28 febbraio 2025: termine per registrarsi sulla piattaforma ACN

Benefici Concreti per i Cittadini

Impatti positivi della NIS 2:

✓ Servizi più affidabili:

- Continuità ospedali e sanità
- Stabilità servizi pubblici
- Energia e acqua garantite
- Trasporti funzionanti

◡ Maggiore fiducia:

- Servizi online sicuri
- Home banking protetto
- E-government affidabile
- Transazioni sicure

■ Dati protetti:

- Protezione dati personali
- Riduzione furti identità
- Sicurezza fascicoli sanitari
- Privacy rispettata

Shield Prevenzione truffe:

- Meno phishing efficace
- Consapevolezza rischi
- Educazione digitale
- Difesa attiva

Conclusioni

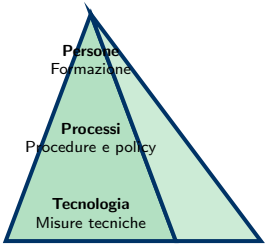
Verso un'Europa digitalmente sicura

Chart Il contesto:

- Minacce in continua evoluzione
- IA che potenzia gli attacchi
- Interconnessione crescente
- Necessità di protezione coordinata

Shield La risposta:

- NIS 2 come framework comune
- Obblighi chiari e misurabili
- Sanzioni deterrenti
- Cultura della cybersecurity



Ecosistema resiliente

Responsabilità condivisa

Pubblico e privato devono collaborare per costruire un ambiente digitale sicuro.

Riferimenti Bibliografici

- Direttiva (UE) 2022/2555 del Parlamento Europeo e del Consiglio
- `https://digital-strategy.ec.europa.eu/it/policies/nis2-directive`
- `https://direttivanis2.eu`
- `https://www.akamai.com/it/glossary/what-is-nis2`
- Decreto Legislativo 4 settembre 2024, n. 138
- `https://www.acn.gov.it` - Agenzia per la Cybersicurezza Nazionale

Grazie per l'attenzione!

? Domande?