CYBER SECURITY

La minaccia Cibernetica

Ordine del giorno

- Introduzione
- Criminalità Cibernetica
- Spionaggio Cibernetico
- Terrorismo Cibernetico
- Guerra Cibernetica
- Hacktivismo
- Tipi di Minacce
- Conclusione

Ordine del giorno

- Introduzione
- Criminalità Cibernetica
- Spionaggio Cibernetico
- Terrorismo Cibernetico
- Guerra Cibernetica
- Hacktivismo
- Tipi di Minacce
- Conclusione

INTRODUZIONE

- Criminalità Cibernetica
  - Attività illegali condotte tramite internet
- Spionaggio Cibernetico
  - Raccolta di informazioni sensibili attraverso la rete
- Terrorismo Cibernetico
  - Uso di tecnologie informatiche per atti di terrore
- Guerra Cibernetica
  - Conflitti tra stati condotti attraverso attacchi informatici
- Hacktivismo
  - Uso di hacking per scopi politici o sociali

Criminalità Cibernetica

- Definizione di criminalità cibernetica
  - Attività criminale che coinvolge un computer
  - Include reti di computer o dispositivi connessi a Internet

TIPOLOGIE DI CRIMINI INFORMATICI

- Cyberestorsione
  - Richiesta di denaro per evitare un attacco informatico preannunciato
- Violazioni del copyright
  - Distribuzione non autorizzata di materiale protetto da copyright
- Vendita online di articoli illegali
- Frodi tramite e-mail e Internet

TIPOLOGIE DI CRIMINI INFORMATICI

- Furto d'identità
- Ransomware
- Cryptojacking
- Cyberspionaggio
- Attacchi Denial of Service (DoS)
- Furto e vendita di dati aziendali

Autori e motivazioni

- Tipi di criminali cibernetici
  - Individui singoli
  - Organizzazioni ben strutturate
- Competenze tecniche elevate
  - Necessarie per eseguire attacchi complessi
- Motivazioni degli attacchi
  - Finanziarie
  - Politiche
  - Personali

Misure di protezione

Uso di software antivirus	• Protegge il sistema da malware e virus
Aggiornamento regolare dei sistemi	• Garantisce la protezione contro le nuove minacce
Formazione sulla sicurezza informatica	• Educazione su come riconoscere e prevenire i rischi
Sensibilizzazione sui rischi del phishing	• Conoscenza delle truffe online comuni

Spionaggio Cibernetico

Definizione di Spionaggio Cibernetico	• Ottenere informazioni riservate senza autorizzazione • Utilizzo di tecniche informatiche
Attori Coinvolti	• Stati-nazione • Organizzazioni criminali • Individui
Obiettivi dello Spionaggio Cibernetico	• Governi • Aziende • Istituzioni finanziarie
Tipi di Informazioni Raccolte	

Tecniche utilizzate

Phishing e Spear Phishing

Email ingannevoli

Inducono le vittime a rivelare informazioni sensibili

Malware

Software dannoso

Installato sui sistemi delle vittime

Rubare dati

Exploits Zero-Day

Sfruttamento di vulnerabilità sconosciute

Nei software

Social Engineering

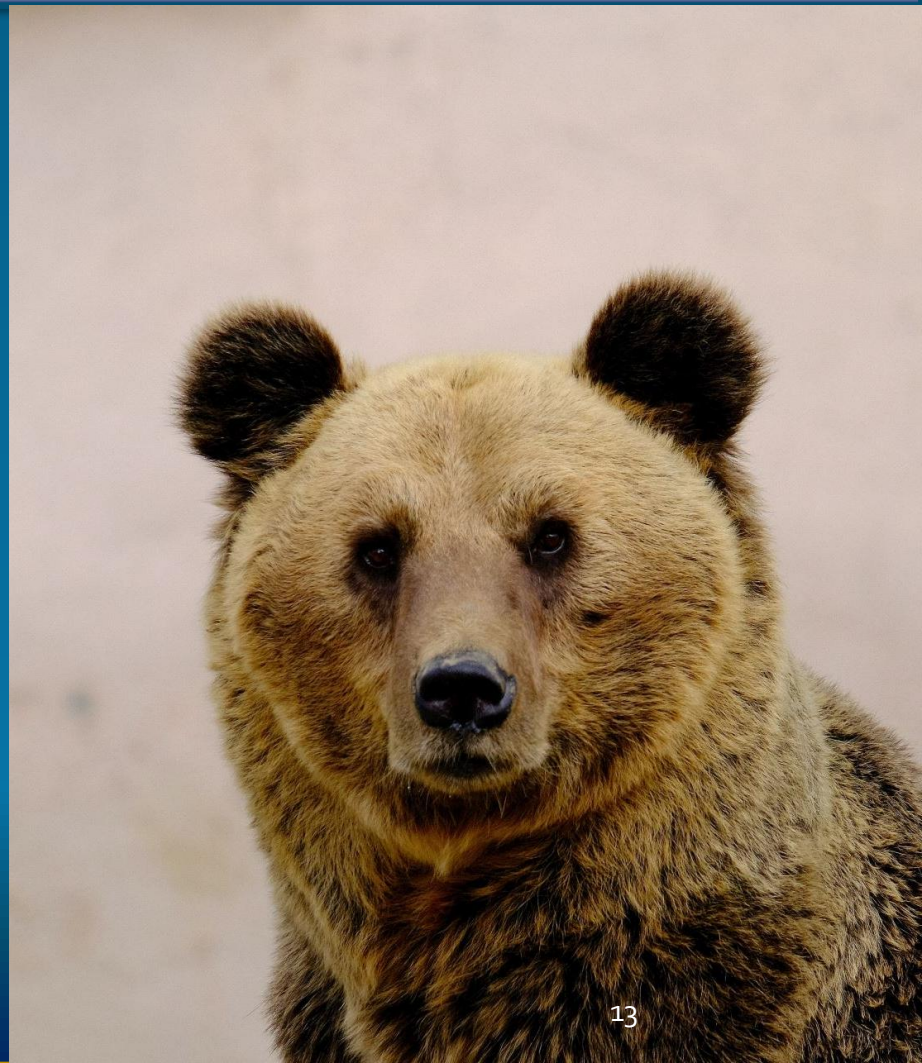
Manipolazione psicologica

Attori coinvolti

- Stati-Nazione
  - Coinvolti in operazioni di spionaggio
  - Obiettivo: ottenere vantaggi geopolitici
- Gruppi di Hacker
  - Sponsorizzati da governi o indipendenti
  - Motivazione: profitto
- Organizzazioni Criminali
  - Utilizzano lo spionaggio per attività illegali
  - Esempi: furto di identità, frode finanziaria

Esempi noti

- APT (Advanced Persistent Threat) Groups
  - APT28 (Fancy Bear) e APT29 (Cozy Bear)
  - Noti per operazioni di spionaggio sponsorizzate dallo stato
- Operazione Titan Rain
  - Serie di attacchi informatici contro gli Stati Uniti
  - Attribuiti a hacker cinesi, iniziata nel 2003



Impatti e conseguenze

- Perdite Economiche
  - Furto di proprietà intellettuale
  - Furto di segreti commerciali
- Danni alla Reputazione
  - Perdita di fiducia da parte di clienti
  - Perdita di fiducia da parte di partner
- Rischi per la Sicurezza Nazionale
  - Compromissione di informazioni sensibili
  - Influenza sulla sicurezza di un paese

Misure di difesa

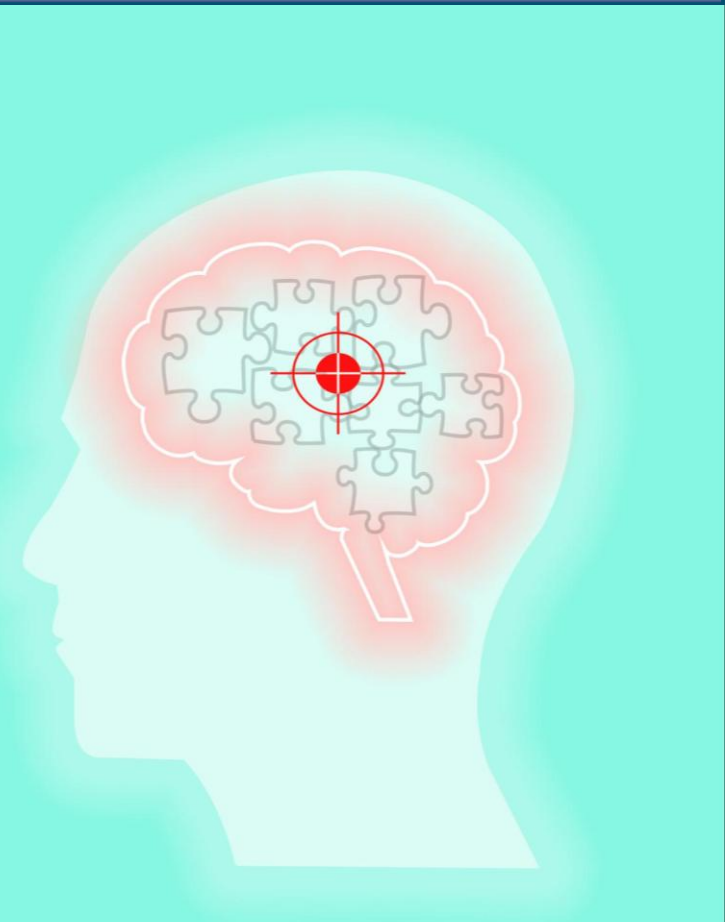
Implementazione di Software di Sicurezza	• Antivirus per proteggere da malware • Firewall per monitorare il traffico di rete • Sistemi di rilevamento delle intrusioni per identificare accessi non autorizzati
Formazione del Personale	• Sensibilizzazione sui rischi di spionaggio cibernetico • Educazione sulle tecniche di social engineering
Aggiornamento Regolare dei Sistemi	• Applicazione di patch di sicurezza • Correzione delle vulnerabilità

Cyberterrorismo

- Definizione di Cyberterrorismo
  - Uso del cyberspazio per atti di terrorismo
  - Attacchi informatici per danni fisici, economici o psicologici
  - Obiettivo di intimidire o coartare governi o società
- Caratteristiche Principali
  - Obiettivi degli attacchi
  - Infrastrutture critiche come reti elettriche e sistemi di trasporto
  - Ospedali e reti di comunicazione
  - Scopo di causare panico, disordine e danni significativi

Tecniche utilizzate

- Malware e Ransomware
  - Interrompono servizi essenziali
  - Estorcono denaro
- Denial of Service (DoS)
  - Sovraccaricano i sistemi
  - Rendono i sistemi inaccessibili
- Phishing e Social Engineering
  - Ottenere accesso non autorizzato
  - Mirano a sistemi sensibili



Propaganda e reclutamento

Utilizzo di Internet per la Propaganda

I terroristi diffondono messaggi radicali online

Obiettivo di influenzare e radicalizzare individui

Reclutamento di Nuovi Membri

Internet come strumento per il reclutamento

Social media e dark web come piattaforme principali

Esempi noti

- Attacco alla rete elettrica ucraina (2015)
  - Ha causato un blackout in diverse regioni dell'Ucraina
  - Attribuito a gruppi di hacker sponsorizzati da stati
- Attacchi a ospedali e infrastrutture sanitarie
  - Numerosi attacchi durante la pandemia di COVID-19
  - Mirati a interrompere i servizi sanitari e a estorcere denaro

Impatti e conseguenze

- Perdite di vite umane
  - Attacchi a infrastrutture critiche possono causare incidenti mortali
- Danni economici
  - Interruzioni di servizi essenziali possono avere un impatto economico significativo
- Panico e Disordine
  - La diffusione di paura e incertezza può destabilizzare società e governi

Misure di difesa

Implementazione di Sistemi di Sicurezza

Utilizzo di firewall per proteggere le reti

Antivirus per prevenire malware

Sistemi di rilevamento delle intrusioni per identificare accessi non autorizzati

Formazione e Sensibilizzazione

Educare il personale sui rischi del cyberterrorismo

Formazione sulle tecniche di social engineering

Collaborazione Internazionale

Cooperazione tra governi per condividere informazioni

Collaborazione con organizzazioni internazionali per strategie di difesa

Guerra Cibernetica

- Caratteristiche Principali
  - Obiettivi degli attacchi di guerra cibernetica
  - Compromettere infrastrutture critiche
  - Reti elettriche, sistemi di trasporto, comunicazioni, strutture militari
  - Causare disfunzioni significative
  - Raccogliere informazioni sensibili
  - Destabilizzare il nemico

Tipi di attacchi

Attacchi a Infrastrutture Critiche

Mirano a servizi essenziali come energia, acqua, trasporti e comunicazioni

Vandalismo Web

Modifica non autorizzata di pagine web

Attacchi DoS per rendere i server inaccessibili

Intercettazione e Alterazione delle Comunicazioni

Intercettazione o modifica di ordini e comunicazioni militari

Raccolta Dati

Spionaggio di informazioni riservate non adeguatamente protette

Propaganda

Diffusione di messaggi politici o fake news per influenzare l'opinione pubblica e creare disinformazione

ATTORI COINVOLTI

Stati-Nazione

- Spesso coinvolti in operazioni di guerra cibernetica
- Mirano a ottenere vantaggi strategici

Gruppi di Hacker

- Possono essere sponsorizzati da governi
- Possono agire indipendentemente

Esempi noti

Operazione Stuxnet

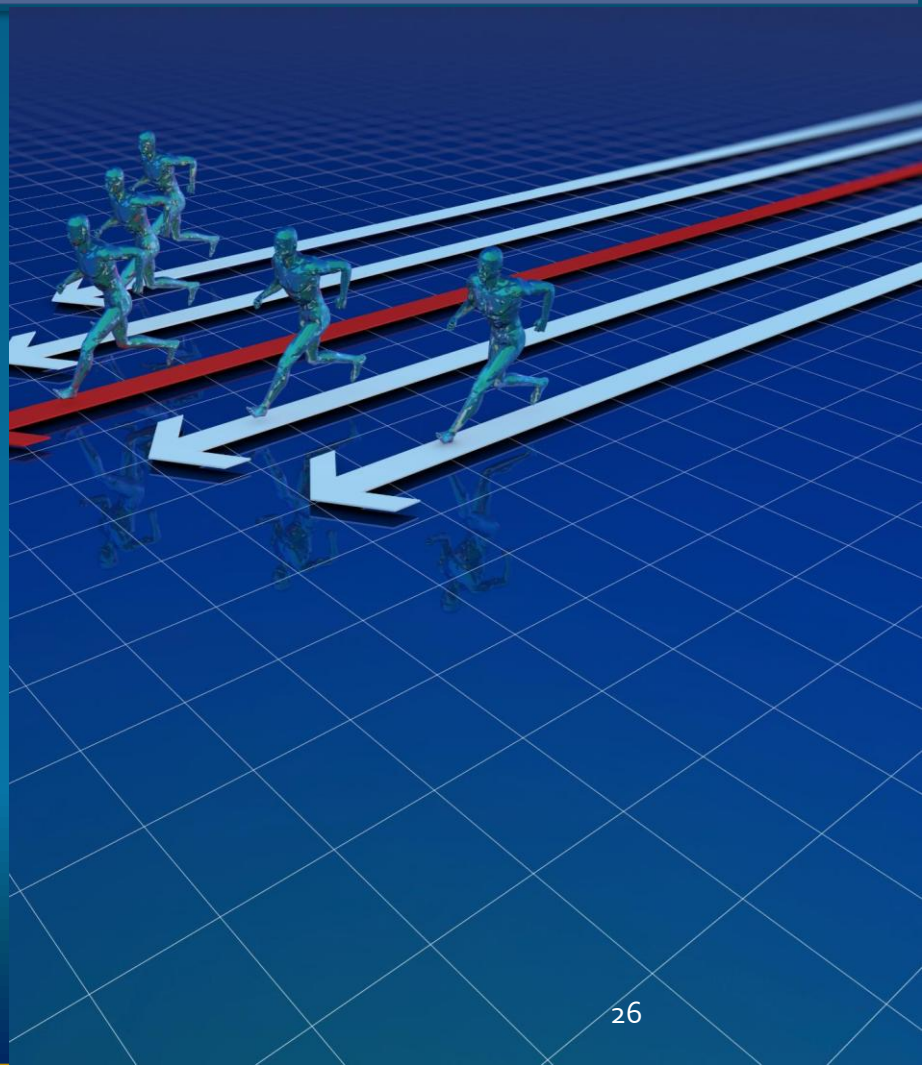
- Attacco informatico contro le centrali nucleari iraniane
- Attribuito agli Stati Uniti e Israele
- Ha danneggiato le centrifughe per l'arricchimento dell'uranio

Titan Rain

- Serie di attacchi informatici contro gli Stati Uniti
- Attribuiti a hacker cinesi
- Iniziata nel 2003

Impatti e conseguenze

- Danni Economici
  - Interruzioni di servizi essenziali
  - Impatto economico significativo
- Rischi per la Sicurezza Nazionale
  - Compromissione di informazioni sensibili
  - Influenza sulla sicurezza di un paese
- Panico e Disordine
  - Diffusione di paura e incertezza
  - Destabilizzazione di società e governi



Misure di difesa

Implementazione di Sistemi di Sicurezza

Utilizzo di firewall

Antivirus

Sistemi di rilevamento delle intrusioni

Formazione e Sensibilizzazione

Educare il personale sui rischi

Insegnare tecniche di social engineering

Collaborazione Internazionale

Cooperazione tra governi

Condivisione di informazioni e strategie di difesa

Hacktivismo

Definizione di Hacktivismo

Forma di attivismo che utilizza tecniche di hacking

Promuove cause politiche o sociali

Origine del Termine

Combinazione di 'hacking' e 'activism'

Uso di competenze informatiche per il cambiamento sociale o politico

Obiettivi degli Hacktivisti

Sensibilizzare l'opinione pubblica su questioni sociali, politiche o ambientali

Prendere di mira governi, aziende o organizzazioni colpevoli di comportamenti scorretti

Tecniche utilizzate

DDoS (Distributed Denial of Service)	• Attacchi che sovraccaricano i server di un sito web • Rendono il sito inaccessibile
Defacement	• Modifica non autorizzata di pagine web • Diffusione di messaggi di protesta
Doxing	• Pubblicazione di informazioni personali • Esporre individui o organizzazioni al pubblico
Rilascio di Documenti Riservati	• Pubblicazione di documenti segreti • Rivelare comportamenti scorretti o illegali

Motivazioni

Senso di giustizia sociale

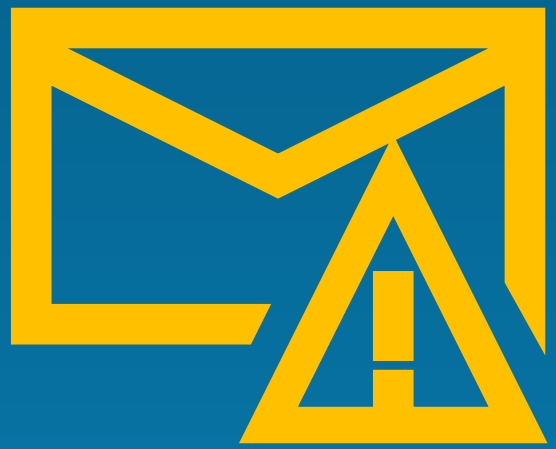
- Desiderio di portare alla luce ingiustizie
- Opposizione agli abusi di potere

Ideali guida

- Trasparenza
- Libertà di informazione
- Diritti umani

Esempi noti

- Anonymous
  - Gruppo di hacktivisti più conosciuti
  - Noto per attacchi contro governi, aziende e organizzazioni
  - Promuove la libertà di informazione e combatte la censura
- WikiLeaks
  - Fondato da Julian Assange
  - Piattaforma che pubblica documenti riservati
  - Espone attività governative e aziendali
- LulzSec
  - Gruppo di hacktivisti noto per attacchi
  - Ha colpito varie organizzazioni
  - Incluso il sito web dell'FBI



Controversie

Visioni contrastanti sull'hacktivismo

- Alcuni vedono gli hacktivisti come paladini della giustizia sociale
- Altri li considerano criminali informatici

Impatto delle azioni degli hacktivisti

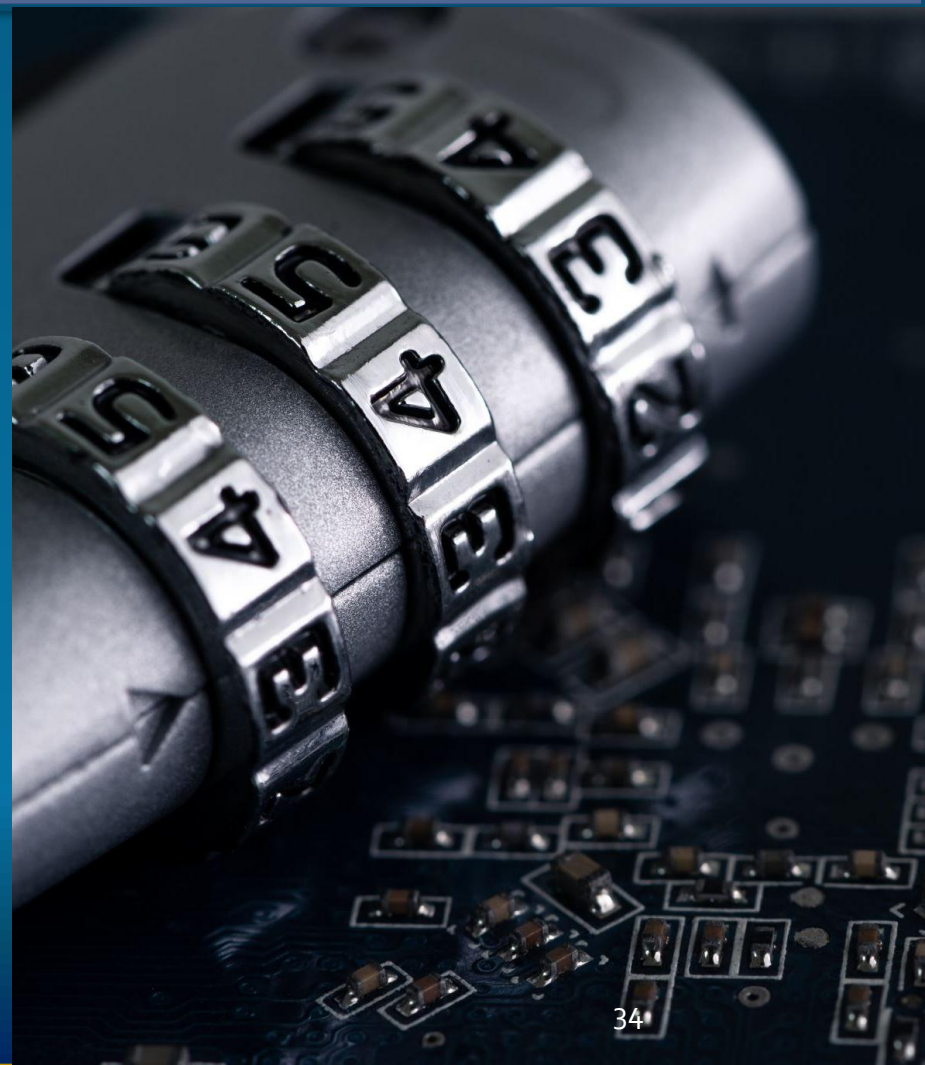
- Possono causare danni significativi
- Violano leggi sulla sicurezza informatica

Misure di difesa

- Implementazione di Sistemi di Sicurezza
  - Utilizzo di firewall
  - Antivirus
  - Sistemi di rilevamento delle intrusioni
- Formazione del Personale
  - Educare i dipendenti sui rischi
  - Insegnare tecniche di social engineering
- Monitoraggio Costante
  - Sorveglianza continua delle reti
  - Rilevamento rapido degli attacchi

Ransomware e Malware

- Ransomware
  - Gli hacker prendono il controllo dei dati
  - Richiedono un riscatto per ripristinare l'accesso
  - Attacchi sempre più complessi e frequenti
- Malware
  - Include virus, worm, cavalli di Troia e spyware
  - Può danneggiare i sistemi
  - Ruba informazioni o prende il controllo dei dispositivi



Ingegneria Sociale e Minacce ai Dati

- Ingegneria Sociale
  - Tecniche che sfruttano l'errore umano
  - Obiettivo: ottenere accesso a informazioni o servizi
  - Esempi comuni: phishing (tramite email) e smishing (tramite SMS)
- Minacce ai Dati
  - Attacchi mirati a ottenere accesso non autorizzato a dati sensibili
  - Tipologie: violazioni dei dati e fughe di dati

Denial of Service e Minacce Internet

- Denial of Service (DoS)
  - Impedisce agli utenti di accedere a dati o servizi
  - Sovraccarica l'infrastruttura di rete
- Minacce Internet
  - Mirano alla disponibilità di Internet
  - Distruzione fisica dell'infrastruttura
  - Censura attiva di siti web

Disinformazione e Attacchi alla Catena di Approvvigionamento

Disinformazione

- Diffusione di informazioni fuorvianti
- Provoca paura e incertezza
- Utilizzo di tecnologia deepfake e bot

Attacchi alla Catena di Approvvigionamento

- Prendono di mira la relazione tra organizzazioni e fornitori
- Organizzazioni vulnerabili a causa della complessità dei sistemi

VARIE TIPOLOGIE DI MALWARE

- Virus
  - Codici che infettano altri file per riprodursi e diffondersi
- Worm
  - Malware che si autoreplica e si diffonde senza bisogno di infettare altri file
- Trojan Horse
- Hijacker
- Keylogger
- Spyware
- Cryptolocker
- Exploit
- Malware Fileless
- Malware Ibrido

Tecniche di attacco

- Phishing
  - Carpire dati sensibili tramite comunicazioni ingannevoli
- Vishing
  - Phishing tramite comunicazioni telefoniche
- IP Spoofing
  - Falsificazione dell'indirizzo IP del computer attaccante
- Web Defacement
  - Alterazione dei dati di un sito web per creare disinformazione
- Backdoor
- Rootkit
- SQL Injection
- Malvertising

Conclusione

- Criminalità Cibernetica
  - Attività illegali condotte tramite internet
- Spionaggio Cibernetico
  - Raccolta di informazioni sensibili senza autorizzazione
- Terrorismo Cibernetico
  - Uso di attacchi informatici per scopi terroristici
- Guerra Cibernetica
  - Conflitti tra stati condotti tramite attacchi informatici
- Hacktivismo
  - Uso di hacking per scopi politici o sociali