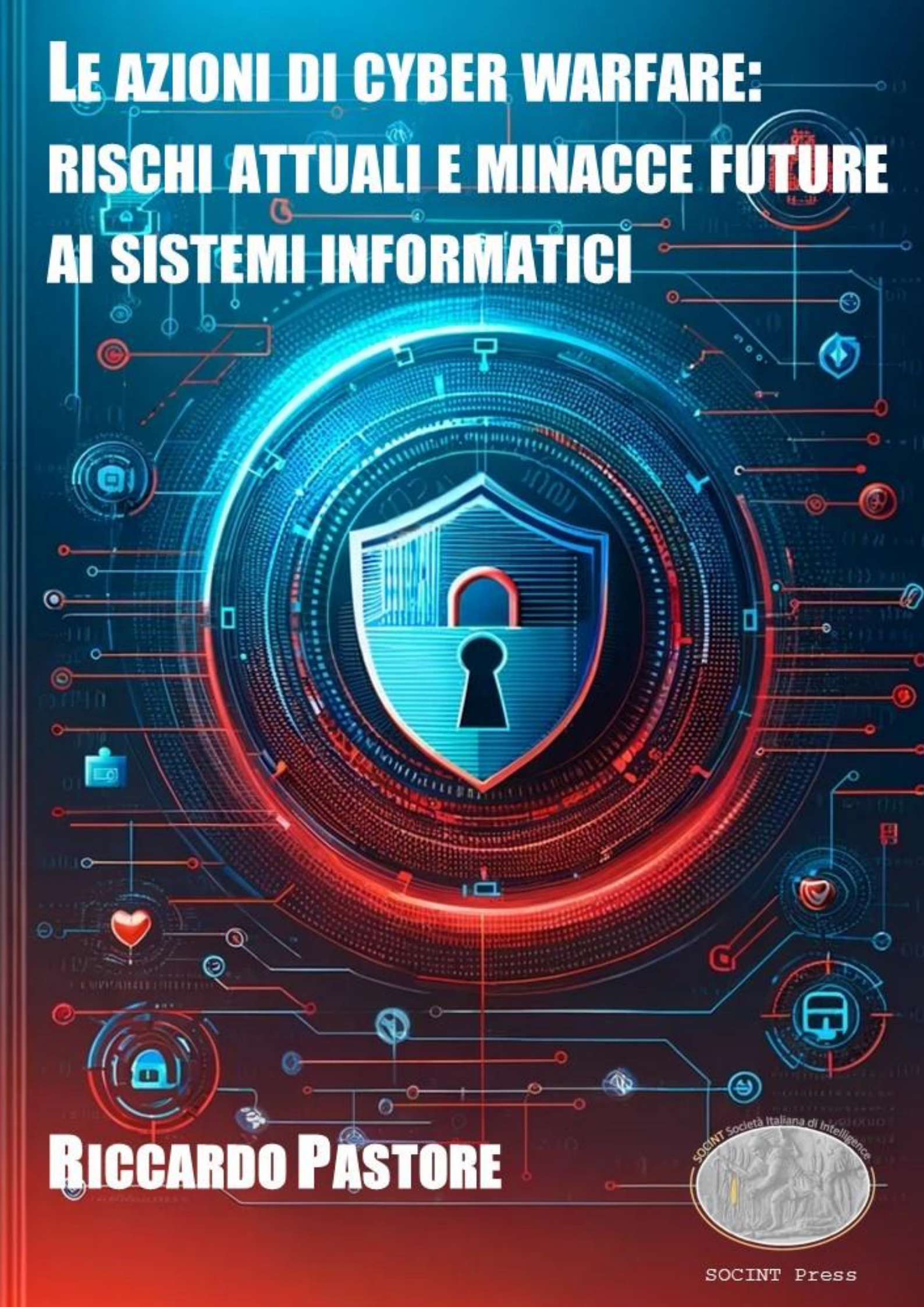
Le azioni di cyber warfare: rischi attuali e minacce future ai sistemi informatici



Riccardo Pastore

SOCINT Press

“Le azioni di Cyber Warfare:
Rischi attuali e minacce future ai sistemi informatici”

Società Italiana di Intelligence
SOCINT Press
c/o Università della Calabria
Cubo 18-b, 7° piano
Via Pietro Bucci
87036 Arcavacata di Rende (CS) –Italia
https://www.socint.org
ISBN 979-12-80111-55-5

Disclaimer
La ricerca presentata in questo elaborato è stata condotta nel corso del 2023 e riflette i dati e le informazioni disponibili fino a tale data. Ogni sforzo è stato fatto per garantire l'accuratezza e la rilevanza dei contenuti, considerando le rapide evoluzioni nel campo della sicurezza informatica. Eventuali discrepanze o variazioni sono attribuibili ai continui sviluppi in questo settore.

"Vi esorto ad essere più innovativi. Quando si tratta di minacce emergenti come la criminalità informatica, la criminalità ambientale e la contraffazione, dobbiamo stare un passo avanti rispetto ai criminali. Dobbiamo anche essere più efficaci nel fermare i flussi di denaro resi possibili dalla corruzione e dal riciclaggio di denaro"[1].

"La cyberwarfare è una minaccia globale che richiede una risposta globale e coordinata da parte della comunità internazionale."

— *Ban Ki-moon, ex Segretario generale delle Nazioni Unite.*

"Il fattore umano è l'anello più debole della sicurezza"[2]

— Kevin D. Mitnick

[1] UNICRI Strategic Engagement in Technology: Supporting The Fight Against Crime And Responding To The Misuse Of Technology

[2] The Art of Deception: Controlling the Human Element of Security

INDICE DEI CONTENUTI

INDICE DELLE FIGURE

INDICE DELLE TABELLE

PRINCIPALI ABBREVIAZIONI

ACL: Access Control List
ACN: Agenzia per la Cybersicurezza Nazionale
AES: Advanced Encryption Standard
AI: Intelligenza Artificiale
APT: Advanced Persistent Threat
BMS: Building Management System
BOT: Robot
C2: Comando & Controllo
CA: Certification Authority
CERT-PA: Centro di Risposta Informatico per la Protezione delle Infrastrutture Critiche della Pubblica Amministrazione
CERT-AgID: Centro di Risposta e Trattamento per la sicurezza ICT dell'Agenzia per l'Italia Digitale
CERT: Computer Emergency Response Team
CFSP: Common Foreign and Security Policy
CI: Controspionaggio
CIIP : Critical Information Infrastructure Protection
CIP : Critical Infrastructures Protection
CIS: Centro di Informatica per la Sicurezza della Repubblica Italiana
CISS: Centro Interforze Studi Strategici Esercito Italiano
CISA: Cybersecurity and Infrastructure Security Agency
CISO: Chief Information Security Officer
CMC: Central Military Commission
CNA: Computer Network Attack
CNAIPIC: Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche
CNCERT/CC: China National Computer Emergency Response Team Coordination Center
CND: Computer Network Defense
CNE: Computer Network Exploitation
CNO: Computer Network Operations
CO: Cyberspace Operations
CSIRT: Computer Security Incident Response Team
CWD: Cyber Warfare Doctrine
CVE: Common Vulnerabilities and Exposures.
DEP: Data Execution Prevention
DCS: Distributed Control Systems
DDoS: Distributed Denial of Service
DIME: Diplomatico, Informativo, Militare ed Economico
DIS: Dipartimento delle Informazioni per la Sicurezza della Presidenza del Consiglio dei Ministri
DLL: Dynamic Link Library
DLP: Data Loss Prevention
DNS: Domain Name System
DoD: Dipartimento della Difesa Americano
DRDoS: Distributed Reflection Denial of Service
EDR: Endpoint Detection and Response
EMET: Enhanced Mitigation Experience Toolkit
ENA: Electronic Network Attack
ENE: Electronic Network Exploitation
ENISA: European Union Agency for Network and Information Security
EPP: Endpoint Protection Platform
ESM: Enterprise Security Management

EU CYBRID: European Union Cyber Rapid Response Teams
Europol: European Union Agency for Law Enforcement Cooperation
FBI: Federal Bureau of Investigation
FDE: Full Disk Encryption
FSB: Federal Security Service
HIDS: Host Intrusion Detection System
HMI: Human-Machine Interface
HTTPS: Hypertext Transfer Protocol Secure
IAM: Identity and Access Management
IC: Infrastrutture Critiche
ICE: Infrastrutture Critiche Europee
ICS: Industrial Control System
IDE: Investimenti Diretti Esteri
IDS: Intrusion Detection System
IO: Information Operations
IoT/IoE: Internet of Things/Everything
IPS: Intrusion Prevention System
IPSec: Internet Protocol Security
ISO: International Organization for Standardization
IW: Information Warfare
JLSF Joint Logistics Support Force
MAC: Mandatory Access Control
MFA: Multi-Factor Authentication
MITM: Man in the Middle
NATO CCD COE: NATO Cooperative Cyber Defence Centre of Excellence
NCSC: National Cyber Security Centre
NIDS: Network Intrusion Detection System
NIPS: Network Intrusion Prevention System
NIS: Network and Information Security
NIST: National Institute of Standards and Technology
NSA: National Security Agency
OAuth: Open Authorization
OCSI: Osservatorio per la Cybersecurity e la Sicurezza delle Infrastrutture Critiche
OPM: Office of Personnel Management
OSE: Operatori dei Servizi Essenziali
OSINT: Open Source Intelligence
OSI-Model: Open System Interconnection Model
PLC: Programmable Logic Controller
RDoS: Ransom Denial of Service
RTU: Remote Terminal Unit
SAML: Security Assertion Markup Language
SCADA: Supervisory Control and Data Acquisition
SIEM: Security Information and Event Management
SMD: Stato Maggiore Difesa
SSL: Secure Sockets Layer
TLS: Transport Layer Security
TTP: Tattiche, tecniche e procedure
URL: Uniform Resource Locator
VPN: Virtual Private Network
Worm: una tipologia di malware

PRINCIPALI LEMMI DI CYBERSECURITY

Advanced Persistent Threat (APT): un tipo di attacco informatico avanzato e mirato, che sfrutta tecniche sofisticate e mirate per penetrare in un sistema.

Audit trail: un registro delle attività di sistema utilizzato per rilevare eventuali violazioni di sicurezza.

Autenticazione: il processo di verificare l'identità dell'utente che cerca di accedere al sistema.

Authentication: il processo di verifica dell'identità dell'utente o del dispositivo.

Authorization: il processo di determinazione dei permessi di accesso dell'utente o del dispositivo.

Autorizzazione: il processo di verificare che l'utente abbia i permessi per accedere a determinati dati o risorse.

Backdoor: una vulnerabilità o una porta segreta introdotta in un sistema informatico per consentire l'accesso non autorizzato o il controllo remoto da parte di un attaccante.

Bitcoin: è una criptovaluta decentralizzata e un sistema di pagamento digitale. È basato sulla tecnologia blockchain e consente transazioni peer-to-peer senza l'intermediazione di una banca centrale o di un'amministrazione governativa.

Blockchain: tecnologia di registrazione distribuita che permette di immagazzinare e condividere dati in modo sicuro e immutabile attraverso una rete di computer interconnessi. Utilizza la crittografia per garantire l'integrità e la trasparenza delle transazioni, eliminando la necessità di un'autorità centrale di controllo.

Botnet: una rete di dispositivi infettati da malware, controllati da un attaccante per effettuare attacchi informatici.

Brute force: L'attacco di forza bruta è un metodo di attacco informatico in cui un aggressore tenta tutte le possibili combinazioni di password o chiavi crittografiche per ottenere l'accesso a un sistema o decifrare dati criptati.

Containerization: una tecnologia di isolamento che separa le applicazioni in contenitori virtuali, impedendo a un eventuale malware di diffondersi tra le applicazioni.

Contingency plan: Un contingency plan nella cybersecurity è un insieme dettagliato di procedure e istruzioni che un'organizzazione deve seguire in caso di incidenti di sicurezza informatica, come violazioni dei dati o attacchi cibernetici.

Crittografia: il processo di codificare i dati in modo da renderli incomprensibili a chi non ha le chiavi di decodifica.

Crittografia anamorfica: area di ricerca che mira a trasformare i dati crittografati in modo che sembrino dati non crittografati, pur mantenendo la loro sicurezza. L'obiettivo è proteggere i dati sensibili senza rivelare la loro natura crittografata.

Crittografia end-to-end (End-to-end encryption): una tecnologia di crittografia che protegge i dati durante la trasmissione, rendendo possibile la lettura solo da parte del mittente e del destinatario.

Dark web: una parte nascosta e non indicizzata di Internet che viene utilizzata per attività illegali o non etiche.

DDoS: Distributed Denial of Service, un attacco in cui un'infrastruttura di computer compromessi viene utilizzata per saturare un sistema o una rete con un traffico in eccesso, impedendone l'accesso.

Deepfake: tecnica di manipolazione multimediale che utilizza l'apprendimento automatico e l'intelligenza artificiale per creare video o audio falsificati in cui le persone possono sembrare dire o fare cose che non hanno effettivamente detto o fatto, sollevando preoccupazioni legate alla manipolazione e alla diffusione di contenuti falsi.

Digital forensics: l'analisi di un sistema o di un dispositivo per raccogliere prove digitali di un attacco informatico.

Digital signature: una firma digitale utilizzata per verificare l'autenticità e l'integrità dei documenti digitali.

Disaster recovery: è l'insieme di politiche, strumenti e procedure utilizzati per recuperare o proteggere un sistema informatico in caso di un evento catastrofico o un attacco cibernetico.

DNS: Domain Name System, il sistema che converte gli indirizzi web leggibili dall'uomo in indirizzi IP utilizzati dalle macchine.

Eavesdropping: è una pratica in cui un individuo o un dispositivo intercetta e ascolta segretamente le comunicazioni tra due o più parti senza il loro consenso. È un'attività invasiva che può essere utilizzata per ottenere informazioni riservate, come conversazioni telefoniche, messaggi di testo, e-mail o altre forme di comunicazione

Encryption algorithm: l'algoritmo utilizzato per convertire i dati in una forma crittografata.

Encryption key: la chiave utilizzata per cifrare e decifrare i dati durante il processo di crittografia.

Encryption: il processo di conversione dei dati in una forma crittografata per proteggerli da accessi non autorizzati.

Exploit: un codice o una tecnica utilizzati per sfruttare una vulnerabilità in un sistema o in un software.

Firewall: un dispositivo o un software che monitora e controlla il traffico di rete in entrata e in uscita e in grado di filtrare il traffico di rete per prevenire gli accessi non autorizzati e gli attacchi informatici.

Flooding attack: Un attacco di flooding è un tipo di attacco informatico in cui l'obiettivo è sovraccaricare un sistema o una rete inviando un elevato numero di richieste o pacchetti di dati, rendendo il sistema o la rete inaccessibile per gli utenti legittimi.

Hacking-as-a-Service (HaaS): un modello di business in cui un'organizzazione o un individuo offre servizi di hacking a pagamento ad altre organizzazioni o individui

Honeypot: un sistema o un dispositivo fittizio utilizzato per attirare gli attaccanti e raccogliere informazioni sulle loro tecniche e obiettivi.

Identity theft: il furto di informazioni personali di un individuo, utilizzato per commettere frodi o accessi non autorizzati.

Incident response: il processo di risposta a un incidente di sicurezza, che prevede la rilevazione dell'incidente, la mitigazione dei danni e la ripristino del sistema.

Incidente di sicurezza: un evento che compromette la sicurezza dei dati, come un attacco informatico o una perdita di dati.

Ingegneria sociale: l'uso di tecniche psicologiche per convincere le persone a fornire informazioni o ad eseguire azioni non autorizzate.

Intelligence Cycle: è un processo sistematico che coinvolge la raccolta, l'analisi, la valutazione e la distribuzione delle informazioni per supportare la presa di decisioni informate e strategiche

Intrusion Detection System (IDS): un sistema di sicurezza che rileva e segnala le attività sospette o non autorizzate sulla rete.

Intrusion Prevention System (IPS): un sistema di sicurezza che blocca le attività sospette o non autorizzate sulla rete.

Kill switch: Un interruttore di disattivazione è una funzionalità incorporata in un malware o in un'applicazione dannosa che consente di interrompere o disattivare l'azione del malware. Può essere utilizzato per fermare o controllare la diffusione di un attacco o per prevenire danni ulteriori**.**

KillDisk: è un tipo di malware che distrugge o corrompe dati critici sul disco rigido di un sistema, rendendoli irrecuperabili. È spesso utilizzato come componente distruttivo in attacchi mirati.

Malvertising: una forma di attacco informatico che sfrutta annunci pubblicitari infetti per diffondere malware.

Malware: un software dannoso progettato per danneggiare o controllare un sistema o un dispositivo.

Man-in-the-middle (MITM): un attacco informatico in cui l'attaccante, interponendosi tra il mittente e il destinatario delle informazioni, intercetta e manipola le comunicazioni tra due parti.

Multi-factor authentication (MFA): un sistema di autenticazione che richiede due o più forme di autenticazione, come una password e un codice di verifica inviato tramite SMS e una scansione biometrica.

Non-proxy: si intente un'applicazione o un dispositivo di rete sta cercando di stabilire una connessione diretta a un server o a una risorsa su Internet senza passare attraverso un server proxy. Questo bypass può essere intenzionale per evitare eventuali restrizioni o blocchi imposti dal server proxy.

OSINT (Open Source Intelligence): o Intelligence delle fonti aperte. È la pratica di raccogliere informazioni da fonti aperte e pubbliche, come siti web, social media, database pubblici e altre risorse disponibili al pubblico. L'OSINT viene utilizzata per ottenere informazioni e conoscenze utili per analisi, indagini e attività di intelligence.

Payload: è una parte di un malware che esegue un'azione dannosa. A differenza di un vettore di attacco (mezzo attraverso il quale il malware viene consegnato), il payload è la parte del malware che effettua l'attività dannosa.

Password manager: un'applicazione che consente di gestire e memorizzare in sicurezza le password.

Patch: un aggiornamento software che corregge una vulnerabilità di sicurezza o bug noti.

Payload: è la parte dannosa o dannosa di un attacco informatico. Può essere un software malevolo, un codice dannoso o un componente che causa danni o svolge un'azione indesiderata sul sistema compromesso.

Peer-to-peer: (P2P) è un modello di comunicazione e condivisione di risorse in cui i partecipanti della rete agiscono sia come client che come server, consentendo la condivisione diretta di informazioni e risorse senza l'intermediazione di un server centrale.

Penetration testing: un test di sicurezza che simula un attacco informatico per verificare la resistenza del sistema.

Phishing: una tecnica di attacco in cui l'attaccante invia un'e-mail fraudolenta o una pagina web falsificata per indurre e convincere l'utente a fornire informazioni personali, cliccare su collegamenti dannosi contenenti codice malevolo che installa un malware.

PowerShell: è un framework e un linguaggio di scripting sviluppato da Microsoft per l'automazione e la gestione di sistemi Windows. È ampiamente utilizzato dagli amministratori di sistema per eseguire operazioni avanzate e gestire risorse di rete.

Ransomware: un tipo di malware che, crittografando i dati, blocca l'accesso ai file o al sistema e richiede un riscatto per ripristinarli.

Ransomware-as-a-Service (RaaS): un modello di business in cui un'organizzazione o un individuo fornisce un software ransomware ad altri soggetti, noti come "affiliati", per scopi di lucro

Ransomware fileless: è una forma di ransomware che non utilizza file eseguibili tradizionali per infettare un sistema. Sfrutta piuttosto le vulnerabilità dei software o i componenti del sistema operativo esistenti per eseguire il codice dannoso direttamente nella memoria del sistema.

Ransom Denial of Service: Ransom Denial of Service (RDoS) è un attacco DoS che prevede un'estorsione di denaro o risorse in cambio del ripristino del servizio o della risorsa informatica resi inaccessibili.

Reflective DLL loading: è una tecnica utilizzata dagli attaccanti per caricare una libreria DLL (Dynamic-Link Library) in modo dinamico nella memoria di un'applicazione senza richiedere l'utilizzo di file DLL esterni.

Reflective dynamic-link library injection: è una tecnica di attacco in cui una libreria DLL viene iniettata in modo dinamico in un processo in esecuzione per eseguire codice malevolo o ottenere l'accesso non autorizzato.

Rete TOR: è una rete anonima e decentralizzata che consente agli utenti di navigare su Internet in modo anonimo attraverso il routing del traffico attraverso una serie di nodi intermedi, rendendo difficile tracciare la fonte delle comunicazioni.

Rootkit: Un rootkit è un insieme di strumenti e tecniche utilizzati da un attaccante per nascondere la presenza di malware o l'accesso non autorizzato su un sistema. Il rootkit può mascherare processi, file e registri di sistema, rendendo difficile la loro rilevazione.

Sandboxing: è una tecnica di sicurezza informatica che isola un'applicazione o un processo in un ambiente controllato, o "sandbox", per prevenire l'interazione dannosa o indesiderata con altri sistemi.

Serial-ethernet: è un termine che si riferisce alla conversione dei dati seriali (comunicazione seriale) in dati Ethernet (comunicazione di rete) per consentire la connessione e la comunicazione tra dispositivi che utilizzano interfacce seriali e dispositivi che utilizzano Ethernet.

SIEM: Security Information and Event Management, una tecnologia che monitora gli eventi di sicurezza in tempo reale per rilevare e prevenire gli attacchi informatici attraverso la raccolta, analisi e monitoraggio delle informazioni di sicurezza provenienti da diversi dispositivi e applicazioni.

Single sign-on (SSO): un sistema di autenticazione che consente all'utente di accedere a più applicazioni con una sola credenziale.

Smishing: una tecnica di attacco in cui l'attaccante per indurre e convincere l'utente a fornire informazioni personali, cliccare su collegamenti dannosi contenenti codice malevolo che installa un malware invia SMS sullo smartphone**.**

Sniffer: un software utilizzato per intercettare e analizzare il traffico di rete.

Social engineering: una tecnica di attacco che sfrutta la manipolazione psicologica delle persone per ottenere informazioni sensibili o riservate.

Spoofing: è una tecnica utilizzata per mascherare o falsificare l'identità o l'origine di una comunicazione, rendendo un mittente o una fonte di dati apparentemente diversi da quelli reali. Ad esempio, l'IP spoofing falsifica l'indirizzo IP di origine di un pacchetto di rete.

SSL/TLS: Secure Sockets Layer/Transport Layer Security, protocolli di crittografia utilizzati per proteggere le comunicazioni su Internet.

Threat intelligence: informazioni sulle minacce che aiutano a prevenire, rilevare e rispondere agli attacchi informatici.

Threat modeling: il processo di identificazione e valutazione delle minacce per determinare quali contromisure di sicurezza implementare.

Typosquatting: è una tecnica in cui un attaccante registra un dominio simile a un dominio legittimo, sfruttando errori di battitura comuni (typos) per indirizzare gli utenti verso siti web dannosi o truffe.

Two-factor authentication (2FA): un sistema di autenticazione che richiede due forme di autenticazione, di solito una password e un codice generato da un'app o inviato tramite SMS.

Virtualizzazione: è una tecnica utilizzata in informatica che permette di creare versioni virtuali o simulate di risorse di sistema, come server, dispositivi di storage, reti o addirittura sistemi operativi completi.

VPN (Virtual Private Network): una rete privata virtuale che utilizza un tunnel criptato per proteggere le comunicazioni tra due o più dispositivi e che consente di navigare in modo anonimo e protetto su Internet.

Vulnerabilità: una falla o una debolezza di un sistema o di un software o di un hardware che può essere sfruttata da un attaccante per compromettere il sistema, per effettuare un attacco informatico.

Watering hole: è una tecnica di attacco informatico in cui un aggressore compromette un sito web legittimo frequentato dai potenziali bersagli, al fine di distribuire malware o raccogliere informazioni sensibili dagli utenti che visitano quel sito senza il loro consenso o conoscenza.

Weaponization: **s**i riferisce alla preparazione di un attacco o di un malware in modo che possa essere utilizzato per danneggiare o compromettere un sistema o una rete.

Zero-day attack: un attacco informatico che sfrutta una vulnerabilità appena scoperta e per la quale non esiste ancora una patch o un aggiornamento disponibile per risolverla.

SINOSSI

La visione olistica dell'ambiente operativo implica una comprensione completa e dettagliata dei differenti ambiti in cui le attività umane e le operazioni militari si svolgono. Queste componenti includono non solo il terreno, il mare, l'aria e lo spazio, ma anche il ciberspazio, una dimensione emergente, trasversale e sempre più importante dell'ambiente operativo moderno. Il ciberspazio si estende oltre le infrastrutture informatiche e le reti di comunicazione, coinvolgendo anche le persone, le organizzazioni e le istituzioni che utilizzano queste tecnologie per interagire e collaborare tra loro. Una visione olistica dell'ambiente operativo deve quindi comprendere anche la sicurezza informatica e la gestione dei rischi nel ciberspazio, riconoscendo che le vulnerabilità e le minacce in questa dimensione possono avere effetti profondi e diffusi in tutto l'ambiente operativo. Ciò richiede una cooperazione internazionale, la formazione continua e la gestione integrata dei rischi in tutte le componenti dell'ambiente operativo, inclusi quelli del ciberspazio.

La Cyber Warfare si lega alla visione olistica dell'ambiente operativo in quanto ne rappresenta una delle componenti fondamentali e necessita di una comprensione globale e integrata per poter essere adeguatamente gestita. Essa consiste nell'utilizzo di tecnologie informatiche, comprese le reti di computer e Internet, per condurre operazioni militari o di intelligence. Queste operazioni includono attacchi cibernetici e altre attività mirate a danneggiare o interrompere le infrastrutture informatiche avversarie, quali sistemi di controllo industriale, reti di telecomunicazioni e di produzione e distribuzione dell'energia.

Le minacce cibernetiche risultano suddivise in diverse categorie e possono essere definite massive o mirate. Una di queste è costituita dai malware, ovvero software malevoli creati per danneggiare o controllare un sistema informatico. Altri tipi di minacce includono le vulnerabilità dei sistemi, le attività di hacking, gli attacchi di

phishing, le attività di sabotaggio e di spionaggio informatico. Ulteriori tipologie di minacce possono essere rappresentate da attacchi cibernetici che si trasformano in attacchi cinetici, che hanno come obiettivo la distruzione fisica di infrastrutture critiche, quali impianti nucleari, dighe elettriche, sistemi di controllo del traffico aereo, sistemi di comunicazione, infrastrutture ospedaliere, o di operatori dei servizi essenziali, come banche e assicurazioni.

La Cyber Warfare è quindi una forma di guerra moderna, operabile da nazioni, organizzazioni o individui, che utilizza le tecnologie informatiche per condurre attacchi nel ciberspazio forieri di ripercussioni negli altri domini della visione olistica dell'ambiente operativo, ma non solo. Può anche essere utilizzata in modo integrato con altre componenti dell'ambiente operativo, come l'uso di droni o di agenti sul terreno (per operazioni di social engineering, di Information Warfare, di propaganda), per massimizzare gli effetti e raggiungere gli obiettivi strategici. Una delle peculiarità della Cyber Warfare è che può essere condotta in modo anonimo e remoto, il che la rende un'arma attraente per i paesi che cercano di esercitare influenza a livello globale.
Inoltre, tra le altre più importanti peculiarità, spiccano l'anonimato degli attaccanti, le difficoltà di identificare in modo preciso gli autori di un attacco e di stabilirne le responsabilità, la necessità di una conoscenza approfondita delle tecnologie informatiche e la velocità di esecuzione con la quale gli attacchi possono essere lanciati e causare danni.

Proprio per questo motivo, nell'era del dato e dell'informazione, la Cyber Warfare rappresenta una delle principali sfide per la sicurezza nazionale e internazionale, nonché una delle maggiori minacce alla sicurezza globale. Una visione olistica dell'ambiente operativo deve quindi comprendere necessariamente la gestione delle minacce cibernetiche e la difesa del ciberspazio, riconoscendo l'importanza di questa componente per la sicurezza globale.

La comprensione e la gestione del ciberspazio risultano pertanto essenziali per una visione olistica dell'ambiente operativo che tenga conto delle complessità e delle sfide della guerra moderna e della sicurezza nazionale.

Negli ultimi decenni la Cyber Warfare è diventata uno dei maggiori temi di attenzione a livello globale, poiché la dipendenza dall'informatica e dalle tecnologie digitali è aumentata a dismisura. Ciò ha portato ad un aumento significativo delle minacce di attacchi informatici e Cyber Warfare, con conseguente necessità di proteggere la sicurezza delle reti e dei sistemi informatici.

L'obiettivo principale di questa tesi è di fornire una panoramica sulla varietà e sull'evoluzione delle principali minacce cibernetico-cinetiche, analizzandone i rischi e le vulnerabilità nell'ambito delle infrastrutture critiche e delle organizzazioni istituzionali e private, esaminarne le sfide che devono essere affrontate per contrastare efficacemente gli attacchi informatici e fornire raccomandazioni pratiche su come affrontare la Cyber Warfare e mitigare i rischi.

Per raggiungere questi obiettivi, la tesi si avvarrà di una metodologia di ricerca basata sulla letteratura scientifica e sull'analisi da fonti aperte (OSINT) di casi di attacchi informatici che hanno avuto luogo negli ultimi anni. Saranno analizzati casi di attacchi informatici di notevole rilevanza per la sicurezza globale occorsi nell'ultimo decennio. In particolare, verranno considerati i seguenti casi attraverso un modello di analisi strutturata che possa mettere a fattor comune la tipologia di target, gli attori coinvolti, le tecniche intraprese per l'attacco, le finalità dello stesso e gli esiti:

1. **Attacco WannaCry (Ransomware):** nel 2017 un worm ransomware si diffuse in tutto il mondo, colpendo le reti informatiche di numerosi ospedali, imprese e istituzioni governative. Il worm sfruttava una vulnerabilità del sistema operativo Windows e chiedeva il pagamento di un riscatto in bitcoin per ripristinare l'accesso ai dati criptati.

2. **Attacco a SolarWinds (Supply Chain):** nel 2020 un gruppo di hacker presumibilmente legati al governo russo attaccò il sistema di gestione delle reti informatiche della SolarWinds, una società di software americana che fornisce servizi a numerose agenzie governative degli Stati Uniti. L'attacco consentì agli hacker di accedere a informazioni riservate e di spiare le comunicazioni interne delle agenzie governative.
3. **Attacco alla rete elettrica Ucraina (OT):** Nel dicembre 2015, la rete elettrica dell'Ucraina subì un attacco cibernetico orchestrato che provocò un blackout elettrico su larga scala, lasciando circa 230.000 persone senza corrente. Gli aggressori utilizzarono il malware BlackEnergy, infiltrandosi nei sistemi tramite una campagna di spear-phishing, per prendere il controllo dei sistemi di controllo industriale e interrompere l'erogazione di energia.
4. **Attacco (Stuxnet) alle Centrali Nucleari Iraniane**: Nel 2010, è stato scoperto un worm informatico noto come Stuxnet, che aveva la capacità di infettare e danneggiare i sistemi di controllo industriale (ICS). L'attacco è stato attribuito a una collaborazione tra Stati Uniti e Israele, con l'obiettivo di danneggiare il programma nucleare iraniano.
5. **Attacco (Netwalker) a ENEL Group**: nel 2020 e nel 2021, la società ha subito un attacco col virus Netwalker e un ulteriore attacco col ransomware Skake/Ekans, che ha portato al furto di circa 5 terabyte di dati (con successiva pubblicazione sul dark web) e alla richiesta di un riscatto di 14 milioni di bitcoin.
6. **Campagne di phishing italiane**: riguarda le campagne di phishing in Italia, in cui gli aggressori inviano e-mail o messaggi di testo ingannevoli fingendosi istituzioni legittime come banche, poste o l'Agenzia delle Entrate. L'obiettivo è ottenere informazioni personali o finanziarie dalle vittime, sfruttando la fiducia verso tali entità e mettendo a rischio la sicurezza delle persone.

La tesi esaminerà anche le sfide future che devono essere affrontate nella lotta contro gli attacchi informatici e le possibili evoluzioni future sui nuovi modelli di attacco, le tecnologie emergenti e le metodologie. Ciò include anche l'importanza della cooperazione internazionale, la necessità di sviluppare strumenti di sicurezza avanzati e di investire nella formazione continua del personale per garantire che tutti siano in grado di riconoscere e rispondere efficacemente agli attacchi informatici.

In sintesi, la tesi intende fornire un sostanziale contributo alla comprensione della Cyber Warfare e degli attacchi informatici. L'analisi dei casi di attacchi informatici occorsi negli ultimi anni costituirà una parte fondamentale della tesi, in quanto consentirà di esaminare le tecniche utilizzate dagli attaccanti, le vulnerabilità sfruttate e le conseguenze degli attacchi.

INTRODUZIONE

Una definizione univoca e puntuale per la *Cyber Warfare* non esiste. Il Glossario del Dipartimento per le Informazioni e la Sicurezza (DIS)[3], che è stato recentemente aggiornato, riporta la definizione di cyberspazio come *L'insieme delle infrastrutture informatiche interconnesse, comprensivo di hardware, software, dati ed utenti nonché delle relazioni logiche, comunque stabilite, tra di essi. Include tra l'altro internet, reti di comunicazione, sistemi attuatori di processo ed apparecchiature mobili dotate di connessione di rete.*

Si definisce pertanto Cyberwar *l'insieme delle operazioni condotte nel e tramite il cyberspace al fine di negare all'avversario – statuale o non – l'uso efficace di sistemi, armi e strumenti informatici o comunque di infrastrutture e processi da questi controllati.*

Include anche attività di difesa e "capacitanti" (volte cioè a garantirsi la disponibilità e l'uso del cyber-space). Può assumere la fisionomia di un conflitto di tipo "tradizionale" – quando coinvolge le forze armate di due o più stati – ovvero "irregolare", quando si svolge tra forze ufficiali e non ufficiali. Può rappresentare l'unica forma di confronto ovvero costituire uno degli aspetti di un conflitto che coinvolga altri dominii (terra, mare, cielo e spazio); in entrambi i casi, i suoi effetti possono essere limitati al cyber-space ovvero tradursi in danni concreti, inclusa la perdita di vite umane.

Inoltre, secondo ENISA (2017), l'Agenzia dell'Unione Europea per la cibersicurezza, il cyberspazio è *l'insieme di beni tangibili e intangibili, dipendenti dal tempo, che memorizzano e/o trasferiscono informazioni elettroniche*. *La sicurezza informatica comprende tutte le attività necessarie per proteggere il cyberspazio, i suoi utenti e le persone interessate dalle minacce informatiche.*

Una tra le definizioni più sintetiche è la seguente: *la Cyber Warfare coinvolge le azioni da parte di uno stato nazionale o di un'organizzazione internazionale volte*

[3] Glossario DIS 2019: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/06/glossario-intelligence-2019.pdf

ad attaccare e tentare di danneggiare i computer o le reti informatiche di un'altra nazione attraverso, ad esempio, virus informatici o attacchi di negazione del servizio[4].

Queste definizioni denotano la complessità, nonché la vastità delle attività, delle operazioni e del potenziale conflitto cyber. Entrando nello specifico, possiamo parlare quindi di "minaccia cibernetica" che il Glossario del DIS definisce come

l'insieme delle condotte controindicate che possono essere realizzate nel e tramite il cyber-space ovvero in danno di quest'ultimo e dei suoi elementi costitutivi. Si sostanzia in attacchi cibernetici: azioni di singoli individui o organizzazioni, statuali e non, finalizzate a distruggere, danneggiare o ostacolare il regolare funzionamento dei sistemi e delle reti e/o dei sistemi attuatori di processo da essi controllati, ovvero a violare integrità e riservatezza di dati/informazioni.

A seconda degli attori e delle finalità, si parla di:

– criminalità cibernetica (cyber-crime): complesso delle attività con finalità criminali (quali, per esempio, la truffa o frode telematica, il furto d'identità, la sottrazione indebita di informazioni o di creazioni e proprietà intellettuali);

– spionaggio cibernetico (cyber-espionage): acquisizione indebita di dati/informazioni sensibili, proprietarie o classificate;

– terrorismo cibernetico (cyber-terrorism): insieme delle azioni ideologicamente motivate, volte a condizionare uno stato o un'organizzazione internazionale.

Tale categorizzazione ha valenza meramente descrittiva, fermo restando che, in concreto, l'azione controindicata spesso non presenta alcuna caratterizzazione peculiare: un'intrusione in un sistema informatico, per esempio, può essere strumentale tanto alla sottrazione di dati per fini di lucro (matrice criminale) quanto ad intenti spionistici o terroristici oppure, ancora, ad attività di c.d. "hacktivism" o "cyber agitation" (l'impiego di computer e di sistemi correlati, con o senza il ricorso a tecniche di hackeraggio, quale forma di protesta ideologicamente motivata).

[4] https://www.rand.org/topics/cyber-warfare.html

La tesi ha come obiettivo di analizzare il contesto attuale della *Cyber Warfare,* con particolare attenzione alle minacce, alle vulnerabilità e ai rischi associati a sistemi informatici industriali e aziendali.

Successivamente, la tesi si concentrerà sulle metodologie di difesa e di prevenzione, con l'obiettivo di evidenziare come mitigare i potenziali impatti della *Cyber Warfare s*ui sistemi informatici industriali e aziendali, nonché sui principali settori del Sistema Paese.

Infine, la tesi formulerà delle ipotesi sulle possibili evoluzioni e sulle sfide future della Cyber Warfare, mettendo in luce come le tecnologie emergenti quali l'Internet delle Cose (IoT), *l'Internet of Everything* (IoE) e l'intelligenza artificiale (AI) potrebbero influenzare l'evoluzione del fenomeno.
Per fare ciò, verranno analizzati vari casi di attacchi informatici occorsi in Italia e nel resto del mondo.

In sintesi, la tesi intende fornire una panoramica sullo stato attuale della Cyber Warfare e sulle strategie di difesa e prevenzione, nonché sulle possibili evoluzioni future di questa forma di conflitto.

CAPITOLO 1 – L'AMBIENTE CIBERNETICO

Come definito nel capitolo introduttivo, la *Cyber Warfare* rappresenta una delle principali sfide della sicurezza internazionale contemporanea, in quanto le minacce cibernetiche costituiscono una seria minaccia per la sicurezza e la stabilità di molte nazioni.
Questo elaborato intende rispondere alla seguente domanda: "Quali sono i rischi attuali e le minacce future per i sistemi informatici a causa delle azioni di *cyber warfare*?" e si concentra, dopo aver definito un perimetro teorico e inquadrato il fenomeno, sull'analisi di una serie di casi di attacchi cibernetici e cinetici alle infrastrutture critiche attraverso l'applicazione di modelli di analisi strutturata che possano mettere a fattor comune la tipologia di target, gli attori coinvolti, le tecniche intraprese per l'attacco, le finalità dello stesso, gli esiti e le difese.
Inoltre, basandoci sui dati raccolti e analizzati, si definiranno gli aspetti principali dei possibili pericoli cibernetici e della difesa del ciberspazio, in particolare analizzando le principali minacce cibernetico-cinetiche e le prospettive future.

Negli ultimi anni, la crescente dipendenza dalle tecnologie IT ha reso i sistemi informatici sempre più vulnerabili agli attacchi, che possono avere conseguenze catastrofiche sulle infrastrutture critiche. Inoltre, la crescente interconnessione tra sistemi informatici a livello globale ha ampliato le possibilità di aggressioni transnazionali, rendendo più difficile individuare e neutralizzare gli autori di tali attacchi.

Quindi, la *Cyber Warfare* viene studiata quale una componente del modello di visione olistica dell'ambiente operativo (rappresentato in figura 1), concentrandosi qui sulla gestione delle minacce cibernetiche e sulla difesa del ciberspazio.

La visione olistica dell'ambiente operativo, così come definito nell'ambiente militare (CJCS, 2014), include una comprensione completa e dettagliata di tutti gli ambiti in cui si svolgono le attività umane e militari, tra le quali spicca il ciberspazio, che è diventato una dimensione emergente e trasversale dell'ambiente operativo moderno e dell'ambiente informativo stesso.

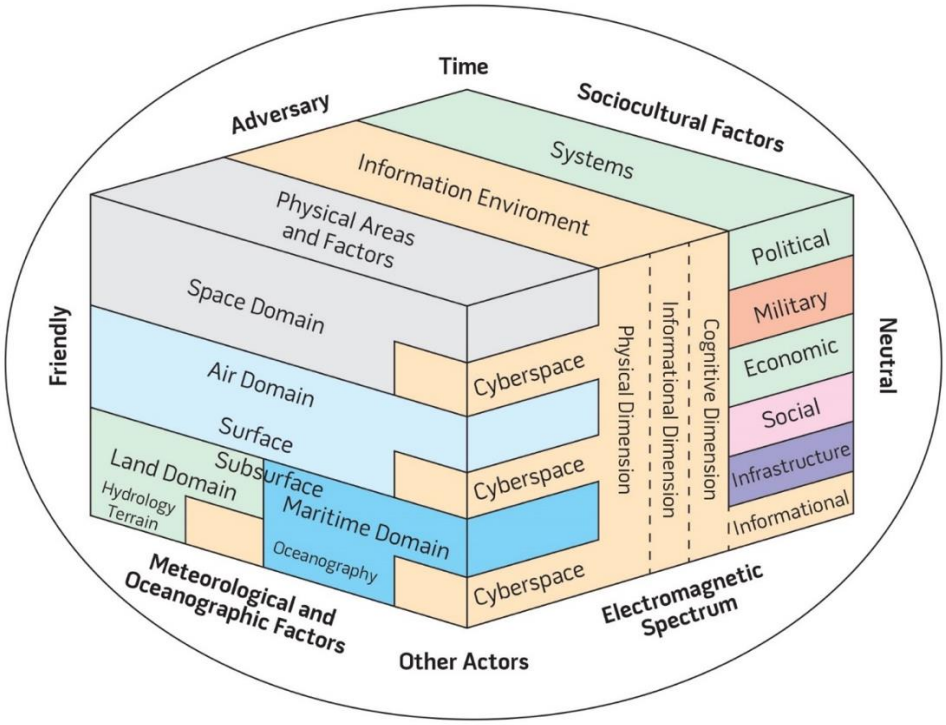


Figura 1 – Visione olistica dell'ambiente operativo ©2014 CJCS Chairman of the Joint Chiefs of Staff

Il ciberspazio e la dimensione umana rappresentano una componente fondamentale della visione olistica dell'ambiente operativo, poiché richiedono una comprensione completa e integrata per essere gestite adeguatamente.

Anche secondo lo Stato Maggiore Difesa (2022), il dominio Cyber, è *quindi caratterizzato dalla sua connotazione virtuale e ubiquitas e risulta trasversale a tutti gli altri domini.*

Così come nelle altre componenti dell'ambiente operativo troviamo i conflitti tradizionali che impattano sulle dimensioni di terra, mare, aria e spazio, all'interno della dimensione *cyber* troviamo le azioni di *cyber warfare*.

Figura 2 - SMD © 2022 - Connotazione virtuale e ubiquitas del dominio Cyber

Le operazioni cibernetiche, che si avvalgono del ciberspazio, dipendono da una rete interdipendente di infrastrutture IT e dipendono da collegamenti e nodi che risiedono nei domini fisici e svolgono funzioni sia nello spazio cibernetico che nei domini fisici. Le attività nello spazio cibernetico possono consentire la libertà di azione per le attività nei domini fisici e viceversa. Queste interrelazioni sono importanti considerazioni in tutto lo spettro delle operazioni cibernetiche, in particolare durante la pianificazione e il coordinamento del targeting nello spazio cibernetico.

Inoltre, le reti possono essere suddivise in enclave con controlli di accesso, crittografia, protocolli diversi o separazione fisica. Tuttavia, nessuno di questi approcci elimina la connettività fisica sottostante; invece, limitano l'accesso. L'accesso alle operazioni cyber può quindi essere influenzato da limitazioni legali, di sovranità, di politica, di ambiente informativo o operative.

Nel manuale JP 3-12 della U.S. Air Force (2023), figura 3, viene descritto l'ambiente cibernetico presentando il modello a tre livelli di cyberspace: rete fisica, rete logica e la dimensione delle persone (gli attori che operano col ciberspazio). Ognuno di questi livelli rappresenta diversi aspetti di cyberspace da cui dovrebbero essere pianificate, condotte e valutate le operazioni cibernetiche.

A questo proposito, ENISA (2017), suddivide ulteriormente la dimensione del cyberspazio in più livelli (figura 4) che rappresentano le interdipendenze tra i vari livelli, ognuno popolato da bisogni ed esigenze differenti.

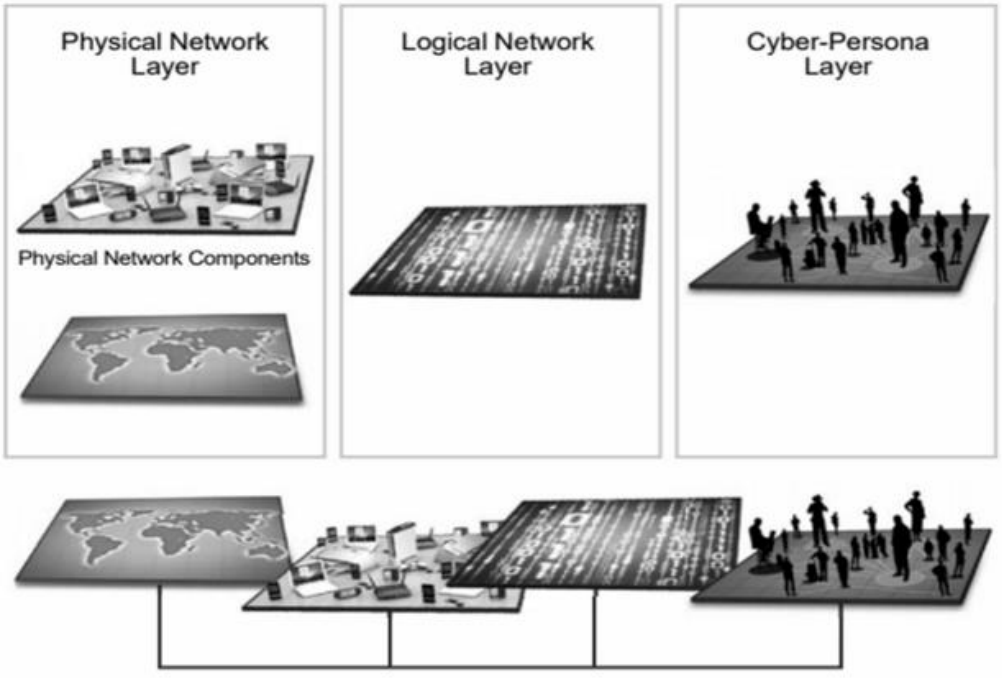


Figura 3 - I tre livelli interconnessi del cyberspazio (JP 3-12) ©2023 AFDP

Come accennato in apertura, tali azioni consistono nell'uso di tecnologie informatiche volte a condurre operazioni di natura civile o militare, tra cui operazioni di spionaggio, attacchi cibernetici per danneggiare o interrompere l'erogazione di servizi afferenti alle infrastrutture informatiche avversarie - di natura privata, pubblica o militare - quali aziende, istituzioni, infrastrutture critiche (IC) e operatori dei servizi essenziali (OSE) del settore energetico, infrastrutturale, finanziario e delle telecomunicazioni, e più in dettaglio, attacchi a portali internet, server, database e banche dati ma anche, a titolo esemplificativo, ai sistemi di controllo industriale, alle reti di telecomunicazioni e di produzione e distribuzione dell'energia. Le operazioni *cyber*, colpendo i centri nevralgici dei paesi, hanno effetto, *non solo su quella che è la dimensione fisica ma anche [su] quella cognitiva*[5].

[5] Video-intervento di Giovanni Gagliano (Stato Maggiore della Difesa) a "CyberSec2023 - Nuovi Domìni, Guerre Ibride e Cooperazione",)

Figura 4 - Livelli di protezione di cybersecurity secondo ENISA © 2017

La *Cyber Warfare* è quindi una forma di guerra moderna che utilizza tecnologie informatiche per condurre attacchi nel ciberspazio con ripercussioni anche negli altri domini dell'ambiente operativo; essendo operabile da nazioni, organizzazioni o individui e in quanto utilizzata in modo integrato con altre componenti dell'ambiente operativo, potrebbe essere considerata come una minaccia ibrida. Per di più, essendo caratterizzata dall'anonimato degli attaccanti, dalle difficoltà nell'identificare gli autori di un attacco (modalità di attribuzione) e dalla velocità di esecuzione, è paragonabile a una delle maggiori minacce alla sicurezza globale; pertanto, richiede una gestione adeguata atta alla difesa del ciberspazio.

Alcuni dei concetti chiave che caratterizzano la minaccia ibrida sono stati definiti dallo Stato Maggiore Difesa nel report "Concetto Scenari Futuri: tendenze e implicazioni per la Sicurezza e la Difesa" (2021) come una tipologia di minaccia complessa che prevede l'uso centralizzato e combinato di tattiche nascoste e non,

nonché di vari tool strategici da parte di attori militari e non, in maniera convenzionale e/o irregolare tra cui gli attacchi *cyber*, le *Information Operations*, la pressione economica, la distruzione di approvvigionamenti energetici e l'appropriazione di infrastrutture critiche. Il report dello SMD continua evidenziando come gli attacchi ibridi siano progettati per sfruttare le vulnerabilità nazionali, puntando all'intero spettro delle funzioni politico, militari, economiche, sociali, informative e infrastrutturali attraverso l'uso coordinato, sistematico e sincronizzato degli *Instruments of Power* DIME (Diplomatico, Informativo, Militare ed Economico), per creare attrito nei confini naturali tra popoli, nazioni e organizzazioni e per minare la fiducia delle persone nei loro governi, nelle loro istituzioni, nei loro alleati e partner. Tra l'altro, citando gli strumenti di potere e l'acronimo DIME, è possibile aggiungere allo stesso anche il suffisso FIL (Finance, Intelligence, Law enforcement), fino a comporre la parola DIMEFIL (Rodriguez C.A. et al, 2020).

Tra le tante definizioni di Infrastrutture Critiche (IC), troviamo quella del Dipartimento della Sicurezza Interna degli Stati Uniti (DHS), che definisce le infrastrutture critiche come *sistemi e reti fisici ed informatici essenziali per la sicurezza nazionale, la sicurezza pubblica, la salute e il benessere economico del paese*[6].
L'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE), nella sua definizione (2007), include *le reti e i sistemi che forniscono servizi essenziali nei settori dell'energia, dei trasporti, delle comunicazioni, dell'acqua e dei rifiuti, nonché quelli di natura finanziaria, di salute e di sicurezza pubblica*[7].
Infine, la Commissione Europea - secondo la Direttiva (UE) 2016/1148 sulla sicurezza delle reti e dei sistemi informativi (nota come NIS2, entrata in vigore il 17 gennaio 2023) - definisce le infrastrutture critiche come *un sistema o un'infrastruttura, o una parte di esso, situato nell'Unione Europea, che è essenziale per il mantenimento di attività vitali della società, della salute, della sicurezza, della sicurezza economica o sociale o dell'ordine pubblico e la cui perturbazione o*

[6] Critical Infrastructure su https://www.dhs.gov/science-and-technology/critical-infrastructure
[7] L'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) su OECD.org

distruzione avrebbe un impatto significativo su uno o più Stati membri[8] . Questa definizione amplia il concetto di infrastrutture critiche rispetto alla precedente Direttiva NIS, includendo non solo le infrastrutture fisiche, ma anche quelle informatiche e digitali. Inoltre, la definizione si concentra sull'importanza di queste infrastrutture per la vita della società, non solo in termini di economia e sicurezza, ma anche di salute e benessere delle persone.

Le infrastrutture critiche diventano quindi elementi essenziali per la funzionalità e la sicurezza di una società e dell'economia, e la loro interruzione o compromissione potrebbe causare un impatto significativo. A titolo esemplificativo, viene riportato uno schema di sintesi della Direttiva (UE) 2022/2555[9] relativa a misure per un livello comune elevato di cybersicurezza nell'Unione europea, meglio nota come **Direttiva NIS2**[10] (Network and Information Systems Directive): identifica una serie di settori delle infrastrutture critiche e degli operatori dei servizi essenziali che sono fondamentali per il funzionamento della società e dell'economia e che potrebbero causare un impatto significativo in caso di interruzione del servizio (Tabella 1). Questi settori sono:

DIRETTIVA (UE) 2022/2555
DEL PARLAMENTO EUROPEO E DEL CONSIGLIO
del 14 dicembre 2022
relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2)

Settori ad alta criticità

I.	Energia: energia elettrica, teleriscaldamento e teleraffrescamento, petrolio, gas, idrogeno
II.	Trasporti: aereo, ferroviario, marittimo e stradale
III.	Bancario: Banche e Infrastrutture dei mercati finanziari
IV.	Sanitario: ospedali e altri servizi sanitari
V.	Acqua potabile
VI.	Acque reflue
VII.	Infrastrutture digitali

[8] Direttiva NIS2: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L1148
[9] https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022L2555
[10] https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=LEGISSUM:4637829

VIII.	Gestione dei servizi TIC (Tecnologie dell'informazione e della comunicazione) (b2b)
IX.	Pubblica amministrazione
X.	Spazio
Altri settori critici	
I.	Servizi postali e di corriere
II.	Gestione dei rifiuti
III.	Fabbricazione, produzione e distribuzione di sostanze chimiche
IV.	Produzione, trasformazione e distribuzione di alimenti
V.	Fabbricazione
VI.	Fornitori di servizi digitali
VII.	Ricerca

Tabella 1 - La DIRETTIVA (UE) 2022/2555

La recente pandemia scatenata dalla diffusione del virus Covid-19, da un lato ha dato una spinta all'innovazione e alla remotizzazione del lavoro e dei servizi, dall'altro ha contribuito all'aumento degli attacchi informatici.

Il Rapporto 2021 OAD (Osservatorio Attacchi Digitali in Italia), pubblicato nell'aprile 2022 (Bozzetti, 2022), riporta il fenomeno Covid-19 come elemento di forte impatto in Italia, come nel resto del mondo. Infatti, il Covid ha avuto ingenti ripercussioni sulle organizzazioni, soprattutto quelle di piccole dimensioni, sia pubbliche che private. La pandemia ha accelerato l'adozione del lavoro da remoto, aumentando l'area di vulnerabilità delle organizzazioni, soprattutto per quanto riguarda la sicurezza digitale.

In particolare, il rapporto OAD 2021 (Bozzetti, 2022) evidenzia l'ampliamento dell'area di vulnerabilità di aziende/enti di piccole dimensioni e i loro relativamente bassi livelli di sicurezza digitale, che hanno impattato

- sui rischi legati ai *collegamenti non protetti tra i dispositivi degli utenti e le applicazioni sui server, sia fisici che virtualizzati, sia on premise che terziarizzati/in cloud.*
- *sull'aumento dell'utilizzo dei dispositivi ICT di proprietà dell'utente, dal PC al tablet e allo smartphone, sui quali raramente sono stati attivati gli opportuni strumenti di sicurezza*

- *sull'argomento Covid-19 che è divenuto la principale esca negli attacchi di phishing ed è un amplificatore di vari tipi di attacchi digitali*.

Inoltre, durante la pandemia, si è verificato un aumento significativo degli attacchi informatici ai sistemi sanitari e di ricerca e, in aggiunta, la fretta e l'urgenza hanno causato numerosi errori nella gestione operativa dei sistemi ICT. Durante questo periodo, inoltre, sono emerse minacce informatiche sempre più sofisticate e difficili da individuare e contrastare, in grado di impattare in maniera significativa sui sistemi informativi.

Il ciberspazio rappresenta oggi un'importante componente del modello di visione olistica dell'ambiente operativo. Infatti, l'interconnessione globale delle reti informatiche e l'uso diffuso di dispositivi mobili e applicazioni online hanno creato un ambiente digitale sempre più complesso e interconnesso, che presenta nuove sfide in termini di sicurezza informatica. Inoltre, la pandemia di COVID-19 ha accelerato l'adozione di nuove tecnologie digitali, aumentando la dipendenza dalle reti e dai servizi online e rendendo più critica la necessità di garantire la sicurezza cibernetica.

CAPITOLO 2 – LE MINACCE E I RISCHI

La sicurezza cibernetica è un tema sempre più rilevante e critico in un'epoca in cui la tecnologia digitale permea ogni aspetto della nostra vita quotidiana.
Essendo una tematica relativamente nuova, solo recentemente le organizzazioni, le istituzioni statali e le organizzazioni internazionali stanno agendo affinché si possano definire e classificare i vari elementi afferenti alla minaccia *cyber*.

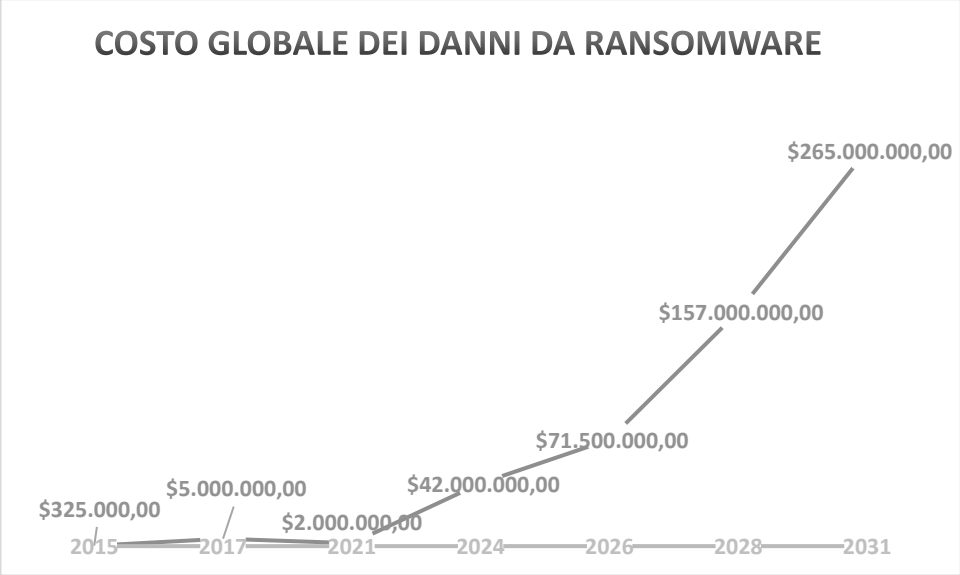
La Relazione Annuale al Parlamento del 2022 pubblicata dal Dipartimento delle Informazioni per la Sicurezza (DIS) evidenzia come la minaccia della criminalità digitale sia in costante evoluzione, con attacchi sempre più sofisticati e mirati che colpiscono sia le istituzioni governative che le imprese e gli individui. La relazione offre uno sguardo dettagliato sulle principali sfide e minacce della sicurezza cibernetica, analizzando anche le misure adottate dal governo italiano per contrastare questi rischi.
A questo proposito, Nunzia Ciardi (Vice Direttore Generale, ACN), nell'intervento occorso in occasione di CyberSec 2023 [11], pone attenzione sull'aumento percentuale significativo degli attacchi informatici alle infrastrutture critiche su base annuale (+ 138%) nonché l'aumento dei ransomware del 460% negli ultimi 4 anni. "Una minaccia insidiosissima che paralizza strutture pubbliche […] blocco di un pronto soccorso, blocco delle radioterapie, ha significato un blocco di prestazioni sanitarie, un impatto sulla vita sanitaria dei cittadini e sulle aziende impatti economici enormi. E anche quando si è in grado di contrastare un attacco ransomware", continua il Vice Direttore Generale, "i tempi di ripristino paralizzano l'attività economica di quell'azienda creando danni ingenti e non solo".

Secondo il rapporto Microsoft, citata in Cybersecurity Ventures (2022) e rappresentata nella tabella sottostante, i danni causati dal ransomware a livello

[11] Video-intervento di Nunzia Ciardi (Vice Direttore Generale, ACN) a "CyberSec2023 - Nuovi Domìni, Guerre Ibride e Cooperazione",

globale ammontavano a 325 milioni di dollari nel 2015 e secondo Braue, citato in KPMG (2022), tabella 2, le previsioni ammonterebbero ad oltre 265 miliardi di dollari entro il 2031. Gli estorsori sono solitamente motivati dal denaro e cercano di ottenere il massimo guadagno possibile dalle loro attività criminose. Solitamente preferiscono attaccare le piccole e medie imprese, che spesso non hanno la protezione adeguata a difendersi dai loro attacchi.

Tabella 2 - Costo globale dei danni da ransomware. Rielaborazione da Cybersecurity Ventures (2022)



Anche la relazione del DIS sottolinea il pericolo rappresentato dalla *cyber warfare*. Poiché questa forma di guerra può essere utilizzata per attaccare le infrastrutture critiche di uno Stato, come le reti di energia elettrica, le infrastrutture di trasporto e le reti di comunicazione, causando gravi danni e disastri, il DIS ha sottolineato l'importanza di sviluppare una capacità di difesa cibernetica efficace per proteggere le infrastrutture critiche del Paese e garantire la sicurezza nazionale.

In aggiunta, la relazione del DIS affronta anche altre minacce per la sicurezza cibernetica mettendo in evidenza la variazione percentuale degli anni 2021 e 2022 (tabella 3), quali:

- il ***cybercrime*** rappresenta una minaccia sempre più diffusa ed è costituito da azioni illegali, con attacchi che vanno dalla frode informatica al ransomware, che blocca l'accesso ai dati dell'utente fino al pagamento di un riscatto, commesse attraverso l'uso improprio di un sistema informatico o telematico.
- il ***cyber-espionage***, ossia attività di spionaggio svolte, di solito, da soggetti legati a uno stato o supportati da esso, che utilizzano sistemi informatici o telematici per la raccolta di informazioni sensibili attraverso *l'hacking* o altre tecniche informatiche.
- il ***cyber-hacktivism***, come l'insieme di azioni condotte tramite l'utilizzo di computer o reti informatiche a scopo sovversivo, finalizzate a promuovere un'agenda politica o sociale attraverso l'uso di attacchi informatici per scopi terroristici.
- Altre categorie di minacce afferenti al dominio cyber: *Cyber terrorism, Cyber sabotage, Cyber Warfare, Cyber theft of intellectual property*, etc.

A questo proposito, nel capitolo precedente, abbiamo introdotto il concetto di "minaccia ibrida". Nell'ambito della *Cyber Warfare* questa si riferisce a un tipo di attacco che combina diverse modalità e tecniche. Gli strumenti, le risorse e le strategie di attacco possono comprendere mezzi sia tradizionali che digitali.
La minaccia ibrida (figura 5) in ambito *cyber* presenta una sfida significativa, poiché richiede un approccio multidisciplinare per combatterla efficacemente. Le tipologie di minacce e di attacchi che analizzeremo nelle prossime pagine, rientrano in questa classificazione (Steingartner, 2021).

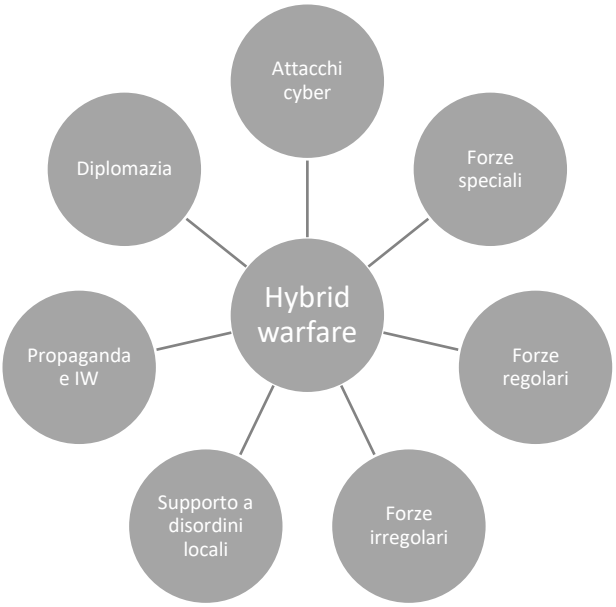
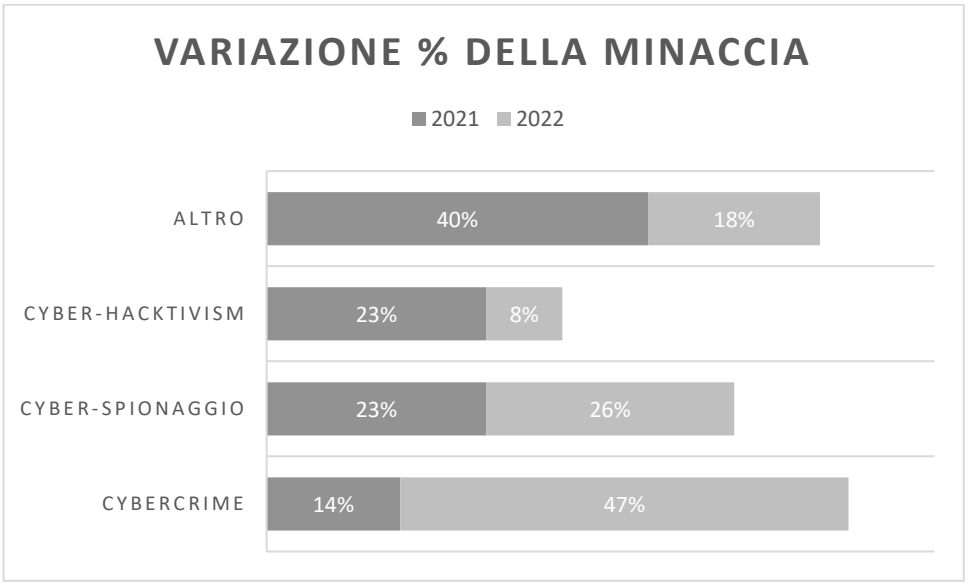


Figura 5 – Rielaborazione di Steingartner (2021) Hybrid warfare

Gli attacchi cibernetici possono essere mirati, ovvero indirizzati a specifici obiettivi, o massivi, oppure diffusi su vasta scala. Gli attacchi mirati sono spesso utilizzati in ambito militare o politico, mentre quelli massivi sono più diffusi in ambito economico o criminale (Relazione Annuale DIS, 2022)

Tabella 3 - Rielaborazione del Rapporto Annuale al Parlamento 2022 a cura del DIS



A questo proposito, anche il rapporto 2021 Osservatorio Attacchi Digitali in Italia (Bozzetti, 2022) classifica gli attacchi *cyber*, indipendentemente da che cosa si attacca e da come, in due macro-categorie, gli attacchi mirati e quelli massivi e li definisce come segue:

- *attacchi "mirati", chiamati sovente anche in italiano "targeted": sono indirizzati specificamente ad un singolo, o ad un gruppo, di aziende/enti; il più delle volte sono attacchi sofisticati, sovente basati su logiche APT, e per i quali gli attaccanti hanno precisi obiettivi da perseguire e in molti casi ben conoscono la realtà informatica del bersaglio;*
- *gli attacchi "massivi", portati ad un grande numero di potenziali bersagli e in molti casi non particolarmente sofisticati, nell'ipotesi che si possa far breccia nelle limitate misure di sicurezza di qualcuno; l'inoltro massivo di phishing che portano in allegato un ransomware è un esempio di questo tipo d'attacco che in Italia, per il grandissimo numero di piccole e piccolissime organizzazioni, è fiorente per quelle con più limitate misure di controllo e scarsa attenzione alla sicurezza digitale.*

A livello europeo, l'ENISA (European Union Agency for Cybersecurity), un'agenzia dell'Unione Europea creata nel 2004 con lo scopo di promuovere un elevato livello di sicurezza dell'informazione nella UE, nel suo ultimo report ENISA Threat Landscape 2022 (ETL) ha identificato 8 principali minacce e 4 categorie di trend emersi negli ultimi anni e che si stanno via via accentuando sempre di più.

Una minaccia informatica è un potenziale evento o azione intenzionale o non intenzionale che può causare danni ai sistemi informatici, alle reti o alle informazioni contenute in essi (Smith, 2020), è "*qualsiasi circostanza o evento con il potenziale di avere un impatto negativo sull'organizzazione, sulle operazioni (comprese missione, funzioni, immagine o reputazione), asset organizzativi, individui, altre organizzazioni, o la Nazione attraverso un sistema informatico*

mediante accesso non autorizzato, istruzione, divulgazione, o modifica di informazioni e/o negazione del servizio" (DoD, 2019)

Per di più, la frequenza e l'impatto determinano quanto siano ancora importanti tutte queste minacce.

- **Ransomware**: una forma di codice malevolo che crittografa i dati dell'utente e richiede un riscatto in cambio della loro decifrazione**.** In figura 6 è rappresentato un tipico diagramma di flusso di attacco.

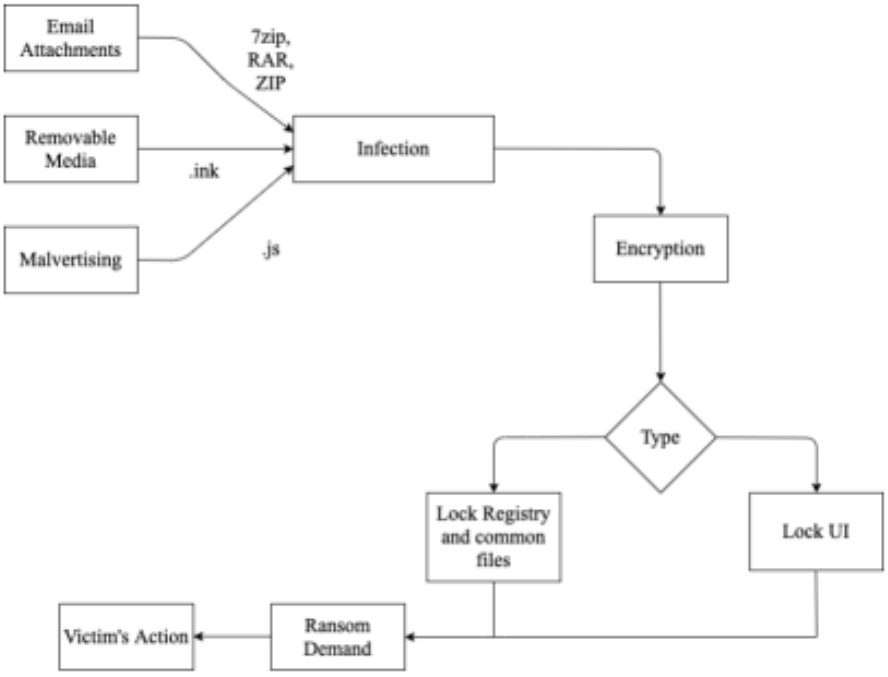


Figura 6 - Schema tipico di un attacco Ransomware © 2022 Kapoor

- **Malware**: software dannoso che può essere utilizzato per rubare informazioni, danneggiare i sistemi o consentire l'accesso remoto ai criminali informatici.
- **Ingegneria sociale (Social Engineering)**: tecniche utilizzate dagli *hacker* per convincere gli utenti a rivelare informazioni riservate o ad installare software dannosi sui loro computer.
- **Minacce contro i dati**: divulgazione non autorizzata di dati e attacchi mirati all'esfiltrazione degli stessi.

- **Minacce contro la disponibilità (*Denial of Service*)**: ovvero un attacco in cui numerosi computer inviano richieste simultaneamente ad un sistema o ad un sito web, sovraccaricandolo e impedendo agli utenti legittimi di accedervi.
- **Internet (*Internet Threats*):** distruzione di infrastrutture, interruzioni e reindirizzamento del traffico Internet
- **Disinformazione – misinformazione**: diffusione volontaria e non di informazioni e notizie fuorvianti o non veritiere allo scopo di modificare la percezione della realtà
- **Attacchi alla catena di fornitura (*supply chain)*:** mirano a compromettere la sicurezza di una catena di approvvigionamento o di produzione, attraverso la compromissione dei fornitori o l'inserimento di malware nella catena di produzione

Tendenze principali

- Gli ***exploit zero-day*** sono la nuova risorsa utilizzata dagli astuti attori delle minacce per raggiungere i loro obiettivi.
- Dopo la guerra Russia-Ucraina è stata osservata una nuova ondata di ***hacktivism.***
- Gli attacchi **DDoS** stanno diventando più grandi e complessi spostandosi verso le reti mobili e *l'Internet of Things* (IoT), che ora vengono utilizzati nella guerra informatica.
- **Disinformazione** e ***deepfake*** abilitati dall'intelligenza artificiale. La proliferazione di bot che modellano i personaggi può facilmente interrompere il processo normativo "avviso e commento[12]", così come l'interazione della comunità, inondando le agenzie governative con contenuti e commenti falsi (Fernandez, 2022).

[12] è un processo attraverso il quale un'agenzia governativa pubblica una proposta di regolamento e invita il pubblico a fornire commenti e suggerimenti su di essa https://www.medialaws.eu/regulating-deep-fakes-in-the-proposed-ai-act/

A queste, è doveroso aggiungere anche le seguenti:

- ***Phishing***: una tecnica di ingegneria sociale che utilizza e-mail fraudolente o siti web contraffatti per convincere le vittime a fornire informazioni personali o a cliccare su link dannosi.
- ***Spear phishing***: un tipo di phishing mirato, in cui gli hacker inviano e-mail fraudolente personalizzate ad utenti specifici, spesso fingendosi una persona fidata o un'organizzazione nota.
- ***Advanced Persistent Threats (APT)*:** attacchi mirati e a lungo termine, in cui gli hacker cercano di penetrare nei sistemi e nelle reti di una specifica organizzazione per rubare informazioni riservate o causare danni.
- **Attacchi alle infrastrutture critiche**: attacchi mirati alle reti e ai sistemi che gestiscono servizi essenziali, come l'energia, l'acqua, il trasporto o le telecomunicazioni, al fine di causare danni o disfunzioni.

Queste tipologie di minacce, che saranno analizzate più dettagliatamente anche nel capitolo di analisi dei casi studio, si aggiungono alle principali categorie di minacce inerenti alla guerra cibernetica (*cyber warfare*), così come definite dalla NATO (Strucl, 2021):

- ***Cyber espionage***: attacchi finalizzati all'acquisizione di informazioni sensibili o segrete da parte di nazioni o organizzazioni rivali, volti a ottenere informazioni riservate di un'organizzazione o di un governo attraverso l'accesso non autorizzato ai loro sistemi informatici (Mazanec, B. M, 2015).
- ***Cybercrime***: attacchi finalizzati a guadagnare denaro o a danneggiare l'immagine di un'organizzazione o di un individuo attraverso il furto di informazioni o l'interruzione dei servizi online.
- ***Cyber terrorism***: attacchi finalizzati a causare danni fisici, sociali o economici attraverso l'uso di strumenti informatici.

- ***Cyber activism****:* attacchi finalizzati a promuovere un'agenda politica o sociale attraverso la diffusione di informazioni o l'interruzione dei servizi online.
- ***Cyber sabotage***: attacchi finalizzati a interrompere o danneggiare le infrastrutture critiche di una nazione o di un'organizzazione, come ad esempio le reti di energia o le infrastrutture di trasporto, con lo scopo di introdurre volontariamente danni o malfunzionamenti nei sistemi informatici di un'organizzazione o di un governo (Janczewski et al., 2008).
- ***Cyber warfare***: attacchi finalizzati a influenzare il corso di un conflitto militare attraverso l'uso di strumenti informatici.
- ***Cyber espionage and theft of intellectual property***: attacchi finalizzati a rubare informazioni riservate o segrete per ottenere un vantaggio competitivo in ambito economico o tecnologico.

Ognuna di queste tipologie, seppur presenti caratteristiche distintive e proprie peculiarità, ha un obiettivo specifico e un modo diverso di essere attuato, ma tutte cercano di compromettere la sicurezza dei sistemi informatici al fine di ottenere informazioni o causare danni.

Inoltre, vi possono essere anche delle attività di attacco di tipo cibernetico che hanno ripercussioni sulle attività cinetiche.
Per attività cinetiche si intendono quelle attività che avvengono nel cyberspazio su apparati di controllo o di gestione che hanno ripercussioni sulla dimensione fisica, come per esempio i sistemi SCADA, DCS o PLC (Setola et al., 2016)[13] . Tuttavia, il problema di base rimane la difficoltà di individuare la direzione e la tipologia di minaccia che potrebbe impattare sia sul dominio civile che su quello militare.
Gli attacchi cibernetico-cinetici combinano tecniche di attacco informatico con azioni fisiche per causare danni e disordini nel mondo reale. Alcune delle tipologie di attacchi cibernetico-cinetici includono:

[13] SCADA (Supervisory control and data acquisition), DCS (Distributed Control System), PLC (Programmable Logic Controller).

- **Attacchi informatici contro i sistemi di controllo industriale (ICS) utilizzati in fabbriche o infrastrutture critiche e attacchi a sistemi SCADA**: questo tipo di attacchi mira ai sistemi di controllo industriale, come quelli utilizzati nella produzione di energia elettrica o nell'approvvigionamento idrico (Irmak et al., 2018).
- **Attacchi a infrastrutture critiche**: questo tipo di attacchi mira a danneggiare o disabilitare le infrastrutture critiche di un paese, come la rete elettrica, i sistemi di trasporto o le reti di comunicazione. (Clarke, 2010).
- **Attacchi a reti militari**: questo tipo di attacchi mira a compromettere le reti informatiche utilizzate dalle forze armate di un paese (Singer et al., 2014).
- **Attacchi a veicoli autonomi**: questo tipo di attacchi mira a compromettere i sistemi informatici utilizzati per controllare veicoli autonomi, come quelli utilizzati nei trasporti pubblici o nell'industria automobilistica (Kuersten, 2017).
- **Attacchi a droni**: questo tipo di attacchi mira a compromettere i sistemi informatici utilizzati per controllare droni utilizzati in missioni militari o di sorveglianza (Lehto, 2021).

ENISA, nel 2022, ha adottato una classificazione delle minacce in 8 categorie (figura 7).

Figura 7 - ENISA Threat Landscape 2022 © 2022 ENISA

Sul fronte occidentale, la NATO ha risposto alle crescenti minaccia cyber attraverso la costituzione nel 2008 del NATO's *Centre of Excellence on Cooperative Cyberdefence* (CDDCOE). Situato in Estonia allo scopo di sviluppare diversi ambiti di *cyberdefence*, si occupa di formazione, ricerca e sviluppo, aspetti legali e di policy. Hagestad II (2012) sostiene che a questa organizzazione debba essere consentito di assumere un ruolo guida nello sviluppo mondiale di strategie e tattiche per mitigare le guerre cibernetiche nel 21° secolo, dal momento che essa possiede l'esperienza, le conoscenze e una forte predisposizione a pensare in termini di contromisure informatiche offensive e difensive, sia tattiche che strategiche.

La UE ha invece affrontato la questione della sicurezza informatica in modo frammentato: talvolta, infatti, sono state lanciate politiche parallele con diversi temi sovrapposti (Klimburg et al., 2011). Sebbene la maggior parte delle potenziali minacce alla sicurezza nazionale informatica degli stati membri possa essere

affrontata utilizzando misure intese a combattere la criminalità e il terrorismo, questo non avviene per altre tipologie di minacce e per specifiche tipologie di attacco che richiedono ingenti risorse e un'attenta pianificazione, di conseguenza è difficile che possano essere perpetrate da attori non statali.

All'interno dell'Unione Europea vi sono due principali aree in materia di sicurezza informatica che hanno particolare rilevanza per la guerra informatica: in primo luogo, vengono utilizzate misure intese a combattere gli attacchi informatici (crimini informatici e cyberterrorismo inclusi) e in secondo luogo, misure intese a sostenere la protezione delle infrastrutture critiche (CIP), delle informazioni critiche (CIIP) e della *Network and Information Security* (NIS2).
Esiste una sostanziale sovrapposizione tra i due settori e spesso gli organi competenti della Commissione si consultano tra loro anche quando non vi è un esplicito obbligo a farlo. Il ruolo di politica estera e di sicurezza comune del CFSP (*Common Foreign and Security Policy*) invece è molto meno sviluppato, in parte a causa della sua natura confidenziale e interdipartimentale, in parte a causa delle difficoltà nell'approcciare un argomento percepito quale questione pertinente ai soli Stati membri.
Le minacce alla sicurezza informatica sono in continua evoluzione e possono presentarsi sotto svariate forme. Comprendere i tipi di minacce esistenti e sapere come prevenirle è fondamentale per proteggere le informazioni e i sistemi sensibili dagli attacchi.

Per far fronte a queste minacce, il Governo italiano ha adottato diverse iniziative di sicurezza cibernetica. La relazione del DIS evidenzia la strategia nazionale per la sicurezza cibernetica, che ha l'obiettivo di proteggere le infrastrutture critiche e promuovere la sicurezza informatica a livello nazionale. Inoltre, sono state sviluppate specifiche linee guida per la sicurezza cibernetica nei settori pubblico e privato, al fine di proteggere le informazioni sensibili e prevenire gli attacchi informatici. Queste si legano alla recente creazione dell'Agenzia per la

Cybersicurezza Nazionale (ACN)[14]. Introdotta in Italia nel 2019 con l'obiettivo di garantire la sicurezza dei sistemi informatici e delle reti nazionali, l'ACN, che è una agenzia governativa, opera all'interno del Dipartimento delle informazioni per la sicurezza (DIS) e ha l'incarico di coordinare, pianificare e implementare le politiche di sicurezza cibernetica dell'Italia. La creazione di questa agenzia è stata necessaria a causa dell'aumento delle minacce informatiche e della vulnerabilità dei sistemi informatici nazionali. Grazie all'ACN, l'Italia può migliorare la propria capacità di prevenire, rilevare e rispondere alle attività cibernetiche ostili, garantendo al contempo la protezione dei propri cittadini e del paese nel suo insieme. La creazione dell'ACN rappresenta un passo significativo nella protezione della sicurezza informatica dell'Italia e dimostra l'impegno del paese per affrontare le minacce cibernetiche sempre più sofisticate.

Finora sono state analizzate svariate tipologie di minacce, di attacchi, di vulnerabilità e di rischi. Nel campo della sicurezza, è bene tenere presenti le differenze tra i lemmi citati e il loro significato (Whitman, 2016)

Il Glossario del DIS (2019) definisce il **rischio** come il potenziale danno per la sicurezza che deriva da un evento, intenzionale o accidentale, in relazione alle vulnerabilità del sistema-Paese o dei suoi settori. Le **minacce**, le **vulnerabilità** e l'eventuale **impatto** costituiscono le variabili principali per valutare l'esistenza e il livello del rischio, al fine di adottare le necessarie contromisure, sia preventive che reattive.
La valutazione del rischio è fondamentale per comprendere il livello di esposizione di un'organizzazione alle minacce e per definire le strategie di protezione da adottare.
Franchina (2018), definisce **l'impatto** e la **probabilità** come elementi che possono essere messi a sistema in una matrice. Il primo, *come la perdita potenziale o il*

[14] https://www.acn.gov.it/

danno a seguito della minaccia secondo dei criteri […] che, come tali, possono essere valutati empiricamente e misurabili qualitativamente e quantitativamente. Il secondo come *la possibilità che l'evento identificato come pericoloso si verifichi realmente.*

Farina (2018), definisce quindi la **minaccia** (figura 8) come "punto di partenza" della valutazione del rischio, intesa come *la possibilità che venga tentato un attacco […], che può insistere su di una "esposizione", […] e sfrutta, ovvero si avvale della debolezza, di una o più "vulnerabilità" […], ed esponendo in tal senso l'organizzazione al rischio, riducendone la sua "sicurezza*.

Farina mette così in luce quanto il *legame esistente tra esposizione, minaccia e vulnerabilità sia molto stretto e da valutare in modo integrato, perché dalla loro combinazione si genera il rischio che può concretizzarsi in danno*.

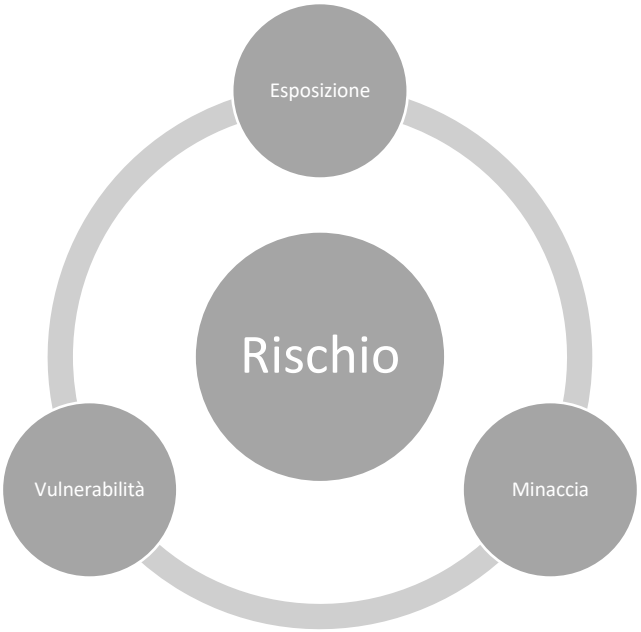


Figura 8 - Rielaborazione di Farina (2018), Il filo logico del rischio.

Inoltre, osservando il "modello base del rischio" (figura 9) definito dalla ISO27005 (2018) e citato da Corrado Giustozzi, illustrato nel corso del Master in Protezione Strategica del Sistema Paese 2020-2021 per SIOI Roma, è possibile introdurre nuovi elementi utili. Esistono quindi degli asset (di un'organizzazione), che hanno

un valore ma anche delle vulnerabilità. All'esterno ci sono delle minacce (di varia natura) che impattano e operano sul valore e che sfruttano le vulnerabilità.

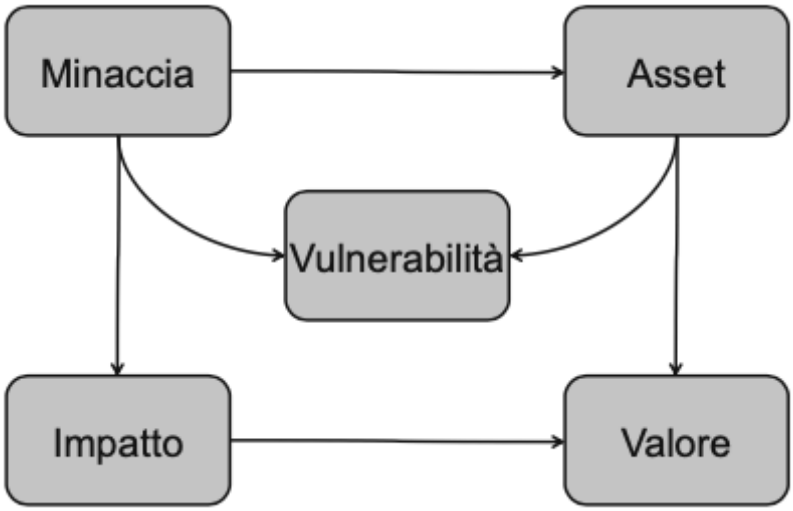


Figura 9 – ISOIEC 27005:2018 - Il modello base del rischio © 2020 Giustozzi

Tassonomia dei principali tipi di attacchi e minacce cibernetici

1. ***Malware***: software dannoso che infetta un sistema informatico con lo scopo di danneggiarlo o di ottenere informazioni sensibili.
2. ***Virus***: un tipo di *malware* che si propaga attraverso la copia di se stesso in altri file o programmi.
3. ***Worm***: un tipo di malware che si propaga autonomamente attraverso le reti informatiche, senza la necessità di essere trasmesso da un file o da un programma infetto.
4. ***Trojan***: un tipo di *malware* che si presenta come un programma utile o interessante per l'utente, ma in realtà contiene funzionalità malevole.
5. ***Ransomware***: un tipo di *malware* che cifra i dati sul computer dell'utente e richiede un riscatto per ripristinare l'accesso ai dati.
6. ***Phishing***: un'aggressione in cui l'attaccante si finge un'entità affidabile per ottenere informazioni sensibili dall'utente, come le credenziali di accesso.
7. ***Spear phishing***: un tipo di *phishing* mirato a una singola persona o a un gruppo ristretto di persone.

8. ***Whaling***: un tipo di phishing mirato a personaggi di spicco, come manager o dirigenti aziendali.
9. ***Pharming***: un attacco in cui l'attaccante dirotta il traffico di rete dell'utente verso un sito web malevolo, al fine di rubare informazioni sensibili.
10. **DDoS**: *Distributed Denial of Service*, quando l'attaccante sovraccarica un sito web o un sistema con una quantità enorme di richieste, al fine di renderlo inaccessibile.
11. ***Man-in-the-middle***: un'azione grazie alla quale l'attaccante si intromette nella comunicazione tra due parti, al fine di intercettare o modificare i messaggi scambiati.
12. ***Zero-day exploit***: un attacco che sfrutta una vulnerabilità sconosciuta del software, prima che il produttore abbia avuto il tempo di rilasciare un aggiornamento di sicurezza.
13. ***SQL injection***: un attacco in cui l'attaccante inserisce del codice malevolo in una *query* SQL, al fine di accedere o modificare i dati presenti nel database.
14. ***Cross-site scripting***: azione con cui l'attaccante inserisce codice malevolo in una pagina web, al fine di rubare informazioni sensibili o di eseguire operazioni dannose.
15. ***Password attack***: un'incursione in cui l'attaccante tenta di indovinare o di violare le credenziali di accesso dell'utente.
16. ***Eavesdropping***: quando l'attaccante intercetta la comunicazione tra due parti, al fine di ascoltare o di rubare informazioni sensibili.
17. **Attacco fisico**: aggressione con cui l'attaccante accede fisicamente al sistema informatico, al fine di ottenere informazioni sensibili o di compromettere il sistema.
18. **Attacchi di infiltrazione (*exploit* e *password cracking*)**:
19. **Attacchi di *sniffing***: consistono nel catturare e analizzare il traffico di rete per ottenere informazioni sensibili come password o dati personali.
20. **Attacchi di *spoofing***: riguardano la falsificazione dell'identità o dell'indirizzo IP al fine di ingannare o eludere i sistemi di sicurezza.

21. **Attacchi di *insider***: sono condotti volontariamente da persone interne all'organizzazione con accesso privilegiato, al fine di danneggiare o sottrarre informazioni sensibili

22. ***Social Engineering*** (Ingegneria Sociale): è inerente l'inganno psicologico e la manipolazione delle persone al fine di ottenere informazioni riservate o accesso non autorizzato ai sistemi.

23. **Minacce persistenti avanzate (APT)**: sono attacchi altamente mirati e sofisticati che spesso provengono da attori statali o gruppi di hacker esperti, che cercano di ottenere un accesso persistente e prolungato alle reti per scopi di spionaggio o sabotaggio.

Tassonomia dei principali attacchi informatico-cinetici

La tassonomia degli attacchi informatici-cinetici comprende diversi tipi di attacchi, tra cui gli attacchi di controllo industriale, gli attacchi di sabotaggio fisico, gli attacchi di interruzione del servizio, gli attacchi di *hacking*, gli attacchi di spionaggio, gli attacchi di guerra elettronica e gli attacchi di cyber-terrorismo. Gli attacchi mirano a compromettere la sicurezza di infrastrutture critiche, compromettendo i sistemi informatici, interferendo con le comunicazioni e causando paura e terrore tra la popolazione. Gli attaccanti utilizzano una varietà di metodi, come l'uso di malware specifici, tecniche di phishing, di exploit delle vulnerabilità dei sistemi, di ingegneria sociale o di *sniffing* dei dati in transito, per compromettere la sicurezza delle infrastrutture critiche.

- **Attacchi di controllo industriale (Industrial Control Systems - ICS**): Gli *Industrial Control Systems* (ICS) sono un insieme di dispositivi di controllo, sistemi e reti utilizzati per gestire e amministrare operazioni critiche e infrastrutture in settori come l'energia, il trasporto, la manifattura, la depurazione dell'acqua, e molti altri. Questi sistemi sono essenziali per la manutenzione, il funzionamento e il monitoraggio di infrastrutture complesse e mission-critical (Stouffer et al., 2015).

- Gli **attacchi ai sistemi di controllo industriale** fanno riferimento a tentativi malevoli di compromissione o manipolazione degli stessi. Queste tipologie di attacchi possono includere tentativi di accesso non autorizzato, sabotaggio, spionaggio industriale o terrorismo. Inoltre, possono avere conseguenze devastanti, come interruzioni del servizio, danni fisici alle infrastrutture, perdite economiche significative e potenzialmente anche perdite di vite umane, per esempio, nei casi di compromissione di apparecchiature mediche (Bengt, 2017).
- **Attacchi di sabotaggio fisico**: prevedono l'uso di metodi fisici per distruggere o danneggiare le infrastrutture critiche. Ad esempio, un attaccante può causare danni fisici a un edificio, a una diga o a un ponte per compromettere la loro funzionalità. Gli attacchi di sabotaggio fisico possono essere combinati con attacchi informatici per aumentare l'impatto dell'attacco.
- **Attacchi di interruzione del servizio**: hanno lo scopo di interrompere i servizi essenziali, come quelli forniti dalle reti di telecomunicazioni, per causare danni all'economia e alla sicurezza nazionale. Gli attacchi possono essere condotti utilizzando malware, attacchi DDoS (*Distributed Denial of Service)* o compromettendo i sistemi di autenticazione.
- **Attacchi di hacking**: prevedono la compromissione dei sistemi informatici per accedere a informazioni riservate o per modificare i dati. Gli attacchi di hacking possono essere condotti utilizzando tecniche di phishing, di exploit delle vulnerabilità dei sistemi, di ingegneria sociale o di sniffing dei dati in transito.
- **Attacchi di spionaggio**: prevedono l'accesso non autorizzato a informazioni riservate per ottenere vantaggi militari, politici o economici. Gli attacchi di spionaggio possono essere condotti utilizzando malware, tecniche di ingegneria sociale o di sniffing dei dati in transito.
- **Attacchi di guerra elettronica**: prevedono l'uso di tecniche di disturbo delle comunicazioni per compromettere la capacità di un'organizzazione di condurre operazioni militari. Gli attacchi di guerra elettronica possono

essere condotti utilizzando jamming delle comunicazioni, interferenze elettroniche o disturbo del segnale GPS.

- **Attacchi di cyber-terrorismo**: prevedono l'uso di tecniche informatiche per causare paura e terrore tra la popolazione. Gli attacchi di cyber-terrorismo possono essere condotti utilizzando tecniche di *hacking*, attacchi DDoS o compromettendo i sistemi di autenticazione.

Il comune denominatore tra queste diverse tipologie di attacchi informatici e cinetici risiede nella capacità di compromettere la sicurezza e la funzionalità delle infrastrutture critiche e delle organizzazioni private. Tutti questi attacchi sono finalizzati a causare danni, interruzioni dei servizi, rubare informazioni riservate o compromettere la capacità di un'organizzazione di svolgere le proprie attività.

Inoltre, tutte le tipologie di attacchi possono essere condotte utilizzando tecniche di ingegneria sociale, come il *phishing*, per indurre gli utenti a fornire informazioni riservate o per compromettere i sistemi. Infine, la maggior parte degli attacchi di successo si basa sulla scoperta e sfruttamento di vulnerabilità insite nei sistemi, evidenziando l'importanza della prevenzione e della protezione contro tutti gli attacchi informatici.

Pur variando notevolmente in termini di metodologia e obiettivi, gli attacchi *cyber* tendono ad avere alcuni elementi comuni:

- **Sfruttamento delle vulnerabilità**: Molti attacchi informatici sfruttano le vulnerabilità dei *software* e dei sistemi informatici, inclusi errori di programmazione, configurazioni non sicure o l'uso di *software* obsoleto (Symantec, 2019).
- **Inganno dell'utente**: Molte forme di attacchi informatici, come il *phishing*, si basano sull'inganno degli utenti per ottenere l'accesso a informazioni sensibili o installare *malware* (NCSC, 2020).

- **Ricorso al *malware***: Molti attacchi informatici utilizzano varie forme di malware, tra cui *virus*, *worm*, *trojan* e *ransomware*, per compromettere i sistemi o i dati degli utenti (Cisco, 2018).
- **Obiettivo di guadagno**: Che si tratti di furto di dati per la vendita sul mercato nero, di estorsioni tramite ransomware o di frodi finanziarie, molti attacchi informatici sono motivati dal guadagno economico (FBI, 2020).
- **Persistenza**: Gli attacchi avanzati persistenti (APT) cercano di mantenere l'accesso a una rete il più a lungo possibile, spesso rimanendo dormienti per mesi o addirittura anni (FireEye, 2020).

Un ulteriore punto, comune alle principali minacce e attacchi, è la condotta della "*cyber operation*" stessa, definita da Teti (2021) in cinque step:

1. Identificazione (*Identification*)
2. Penetrazione (*Penetration*)
3. Presenza (*Presence*)
4. Sfruttamento (*Exploitation*)
5. Danno (*Harm*)

A tal proposito, sebbene non esista un consenso universale sulla nomenclatura e sulle caratteristiche di questi passaggi e come vengano definiti o suddivisi potrebbe variare leggermente a seconda delle fonti.

Un modello comune per lo studio di attacchi mirati include sette fasi (Hutchins et al., 2011) ed è basato su un concetto militare tradizionale della *kill chain* (U.S. Air Force, 2021). La dottrina militare statunitense, infatti, definisce le fasi di questo processo come: individuazione, localizzazione, tracciamento, mira, ingaggio, valutazione (F2T2EA[15]). Questo è un processo integrato, *end-to-end*, descritto come una "catena" perché qualsiasi carenza interromperà l'intero processo. Questo modello, denominato "*Cyber Kill Chain*", sviluppato nel 2011 da LockHeed

[15] F2T2EA (Find, Fix, Track, Target, Engage, Assess) è un modello di processo utilizzato nell'ambito della sicurezza informatica per identificare e rispondere alle minacce. Comprende fasi come la ricerca delle minacce, la risoluzione dei problemi, il monitoraggio, l'individuazione del bersaglio, il coinvolgimento attivo e la valutazione delle azioni intraprese.

Martin, è definibile come un processo sistematico per individuare e coinvolgere un avversario al fine di ottenere effetti desiderati e prevede le seguenti fasi:

1. (*Reconnaissance*) Ricognizione: Raccogliere informazioni sul bersaglio.
2. (*Weaponization*) Armamento: Creare o preparare un'arma digitale, detto *payload*, che contiene codice malevolo e/o tool malevoli.
3. (*Delivery*) Consegna: Inoltro dell'arma al bersaglio, ad esempio tramite e-mail o tramite un *exploit.*
4. (*Exploitation*) Sfruttamento: di una o più vulnerabilità per ottenere accesso non autorizzato.
5. (Installation) Installazione: del malware e/o degli strumenti di controllo a distanza.
6. (C2) Comando e Controllo: Stabilire un canale di comunicazione con il sistema compromesso al fine di permetterne la compromissione o l'esfiltrazione di dati attraverso il canale "aperto" tra attaccante e attaccato.
7. (*Actions on Objectives*) Azioni sugli obiettivi: Effettuare azioni finali, come l'esfiltrazione dei dati o il danneggiamento del sistema.

CAPITOLO 3 – GLI ATTORI

Nell'era digitale, una vasta gamma di minacce informatiche, provenienti da varie parti del mondo, mette costantemente alla prova le nostre difese cibernetiche. In particolare, le organizzazioni criminali e i gruppi di *hacker* sono diventati attori sempre più significativi nel panorama della sicurezza informatica. Questi attori non solo posseggono le competenze tecniche per sfruttare le vulnerabilità dei sistemi informatici, ma sono anche motivati da una varietà di obiettivi, che possono spaziare dal guadagno economico alla destabilizzazione politica.

Questo capitolo mira a fornire un'analisi approfondita di questi principali attori, esaminando le loro motivazioni, le loro tecniche e le loro strategie. Dagli studi effettuati saranno analizzate le diverse tipologie di organizzazioni criminali coinvolte nella cybercriminalità.

Anche il report ENISA (2022) evidenzia come vi sia un aumento crescente delle capacità offensive, sia nello sfruttamento di vulnerabilità non ancora note o variazioni continue ai nomi e alle composizioni dei gruppi criminali, in modo da poter depistare le indagini ed evitare l'applicazione di leggi o sanzioni, sia nell'introduzione di nuovi modelli di business quali *l'hacking-as-a-service* e infine una crescente capacità di attacchi a catena.
Dati questi propositi, dagli studi effettuati sull'identificazione degli autori degli attacchi è emerso che vi sono differenti tipologie di attori che possono essere impiegati nella conduzione di attacchi.
Non esistono solo i cosiddetti hacker che, secondo quanto riportano Kizza (2013) e da Andress et al. (2014), a loro volta possono essere distinti in "*white* hat", "*black hat*" e i "*grey hat hacker*", ma la galassia cyber è ben più popolata. Tra questi è possibile trovare:

- **Gruppi sponsorizzati dagli stati (*State-sponsored groups*)**
- **Organizzazioni criminali**
- **Cyber-mercenari**
- **Competitor hacker**
- **Hacker tradizionali**
- **Hacktivisti**
- **Terroristi**
- **Estorsori**
- **Insider**

Tabella 4 - Tipologie principali di hacker

White Hacker	Grey Hacker	Black Hacker
Professionisti della sicurezza informatica che utilizzano le loro competenze per scopi legali e etici, come testare e migliorare la sicurezza dei sistemi informatici.	Operano in una zona grigia etica e legale e mossi da finalità benigne o altruistiche con lo scopo di far emergere falle e vulnerabilità.	Utilizzano le loro competenze per scopi illegali o malevoli, come il furto di dati, la distruzione di infrastrutture informatiche o la diffusione di malware.

Gruppi sponsorizzati dagli stati (*State-sponsored groups*)

Questi sono gruppi che sono sostenuti finanziariamente e logisticamente da uno stato nazionale, e il loro obiettivo principale è di attaccare altri stati o organizzazioni in conflitto con il loro sponsor. Gli obiettivi possono variare, ma possono includere il furto di informazioni sensibili o la destabilizzazione degli assetti del nemico. Secondo un rapporto sulle minacce informatiche future alle infrastrutture critiche (Badhwar, 2021), i gruppi sponsorizzati dallo stato sono noti per utilizzare tecniche di hacking sofisticate e strumenti personalizzati per ottenere accesso ai sistemi della loro vittima e rimanere nascosti il più a lungo possibile.

Caratteristiche:

- Hanno risorse finanziarie e tecniche significative a loro disposizione
- Sono spesso altamente sofisticati e utilizzano tecniche avanzate di *hacking* e di manipolazione dell'opinione pubblica

- Possono agire con una certa impunità, poiché hanno la protezione del loro stato sponsor.

I gruppi sponsorizzati dagli stati sono tra gli attori più sofisticati e avanzati nel campo della *Cyber Warfare,* in grado di utilizzare risorse finanziarie, tecnologiche e umane di alto livello.
Tra le altre peculiarità della *Cyber Warfare* e delle azioni offensive, vi è l'anonimato degli attaccanti e la difficoltà di identificare gli autori degli attacchi.
Una delle tecniche maggiormente utilizzate per occultare l'origine degli indirizzi IP di provenienza consiste nella tecnica degli *hop points*. Teti (2018) lo definisce come *il percorso dei salti che i dati devono compiere per giungere a destinazione. Per cercare di mascherare l'indirizzo IP del computer da cui parte un attacco, si cerca di transitare su diversi dispositivi attivi di rete (router, web server, ftp server, etc.), facendo in modo che l'IP originario si perda nella miriade dei sistemi utilizzati per giungere sul sistema della vittima prescelta.*

Secondo un report pubblicato dall'azienda Radware (2019), i principali attori di questo tipo sono Russia, Cina, Iran e Corea del Nord, con obiettivi e finalità diverse.

La Russia, ad esempio, ha dimostrato di utilizzare tattiche di disinformazione, propaganda e attacchi informatici per destabilizzare governi, organizzazioni elettorali e infrastrutture critiche. Inoltre, la Russia sembra utilizzare la *Cyber Warfare* come strumento di politica estera per raggiungere i propri obiettivi di sicurezza nazionale.

La Cina, d'altra parte, è stata associata a numerosi attacchi informatici finalizzati alla raccolta di informazioni riservate e alla proprietà intellettuale di altri paesi, in particolare nei settori dell'energia, delle tecnologie dell'informazione e delle telecomunicazioni e della difesa (Teti, 2018).

L'Iran sembra utilizzare la *Cyber Warfare* come strumento di deterrenza e rappresaglia contro i propri avversari, con attacchi diretti a infrastrutture critiche e

organizzazioni governative. Secondo una relazione del 2019 del Dipartimento della Difesa degli Stati Uniti, l'Iran ha sviluppato una capacità di attacco informatico sofisticata e continua a migliorare le proprie tecniche.

Infine, la Corea del Nord sembra utilizzare la guerra cibernetica come mezzo per raccogliere informazioni sensibili e generare entrate monetarie. Secondo una relazione pubblicata dal gruppo di sicurezza cibernetica FireEye (2020), la Corea del Nord ha condotto numerosi attacchi di *phishing* per rubare criptovalute, compresa la campagna WannaCry del 2017.

In generale, i gruppi sponsorizzati dagli stati mirano a raggiungere obiettivi politici, militari o economici, spesso attraverso l'acquisizione di informazioni sensibili o il danneggiamento delle infrastrutture critiche degli avversari (Janczewski, 2007). Inoltre, tali gruppi possono utilizzare il *cyberwarfare* come mezzo per estendere la propria influenza e il proprio potere a livello internazionale.
I servizi di intelligence sono gruppi che lavorano per governi o organizzazioni governative, con lo scopo di acquisire informazioni strategiche e sensibili su altri paesi, organizzazioni o individui, che possono essere utilizzate per prendere decisioni politiche, militari o economiche. Questi gruppi utilizzano anche tecniche di *Cyber Warfare* per acquisire informazioni e infiltrarsi in obiettivi sensibili.

I tratti caratteristici dei servizi di intelligence includono la segretezza delle loro attività, la loro struttura gerarchica e il loro accesso a risorse e tecnologie avanzate. Gli obiettivi principali dei servizi di intelligence sono la raccolta di informazioni e la protezione degli interessi del proprio paese o organizzazione. Tuttavia, a volte possono anche essere coinvolti in attività di spionaggio industriale o di sabotaggio.

Principali *State-sponsored groups*[16]

Seppur di difficile attribuzione a uno Stato ben preciso, gli studi effettuati hanno permesso di stilare un nutrito elenco di gruppi afferenti a svariati paesi, per esempio Iran, Cina, Corea del Nord e Russia. La tabella sottostante intende rappresentare la vastità del fenomeno nonché le finalità di alcuni dei più famosi gruppi.

Tabella 5 - Principali gruppi APT

Iran	APT39, APT35, APT34, APT33
Cina	APT41, APT40, APT31, APT30, APT27, APT26, APT25 (Uncool, Vixen Panda, Ke3chang, Sushi Roll, Tor), APT24 (Pitty Tiger), APT23, APT22 (Barista), APT21 (Zhenbao), APT20 (Twiky), APT19 (Codoso Team), APT18 (Wekby), APT17 (Tailgator Team, Deputy Dog), APT16, APT15, APT14, APT12 (Calc Team), APT11, APT10 (Menupass Team), APT9, APT8, APT7, APT6, APT5, APT4 (Maverick Panda, Sykipot Group, Wisp), APT3 (UPS Team), APT2, APT1 (Unit 61398)
Corea del Nord	APT38, APT37, APT28 (Tsar Team), APT32 (OceanLotus Group).
Russia	APT28 (fancy Bear), APT29 (Cozy Bear), APT12 (Comment Crew), APT10 (Red Apollo), Sandworm Team.

Dalla tabella 5 notiamo quindi che vi sono svariati gruppi di hacker che si occupano di spionaggio e raccolta di informazioni a fini politici, militari e commerciali. Ognuno con delle proprie peculiarità, finalità e obiettivi specifici. A questo proposito, *Fancy Bear* è legato al GRU russo e si occupa di spionaggio e raccolta di informazioni politiche e militari. *Cozy Bear* è legato al FSB russo e si occupa di spionaggio a fini politici, militari e commerciali. *Sandworm* Team è legato all'intelligence militare russa e si occupa di spionaggio e sabotaggio a fini politici e

[16] MANDIANT - Advanced Persistent Threats (APTs) https://www.mandiant.com/resources/insights/apt-groups

militari. APT12 è legato all'esercito cinese e si occupa di spionaggio a fini politici e militari, principalmente contro Stati Uniti e Giappone. Infine, APT10 o *Red Apollo* è legato al Ministero della Sicurezza di Stato cinese e si occupa di spionaggio a fini commerciali, con particolare interesse per il settore della tecnologia e dell'industria manifatturiera.

Per quanto riguarda quelli cinesi, APT10, anche noto come *Stone Panda*, è un gruppo cibernetico sponsorizzato dallo stato cinese noto per le sue attività di hacking contro obiettivi statunitensi e giapponesi, con l'obiettivo di rubare proprietà intellettuale e informazioni sensibili. APT40 è invece noto per la sua attività di spionaggio industriale contro aziende del settore navale, mentre APT41, anche conosciuto come *Winnti*, ha attaccato obiettivi asiatici e statunitensi per rubare proprietà intellettuale e diffondere malware. Infine, APT27, noto anche come *Emissary Panda*, ha attaccato obiettivi governativi, militari e industriali in tutto il mondo per la raccolta di informazioni e il furto di proprietà intellettuale.

Tra quelli iraniani invece, APT33, anche noto come *Elfin*, è un gruppo cibernetico sponsorizzato dall'intelligence iraniana, che si concentra sull'attacco ad aziende del settore energetico, militare e delle infrastrutture critiche in Europa, Medio Oriente, Asia e America. APT34, anche noto come *OilRig*, è un altro gruppo cibernetico sponsorizzato dall'intelligence militare iraniana, che si concentra sull'attacco ad aziende del settore petrolifero e del gas, istituzioni governative e media in Europa, Medio Oriente, Asia e America. APT39, anche noto come *Chafer*, è un gruppo cibernetico sponsorizzato dai servizi di intelligence iraniani, che si concentra sull'attacco ad aziende del settore aerospaziale, tecnologia, telecomunicazioni e istruzione in Medio Oriente, Asia e America.

Infine, tra quelli della Corea del Nord, troviamo il *Lazarus Group*, noto anche come *Hidden Cobra*, Bureau 121 o APT38, uno tra i principali gruppi di *Cyber Warfare* della Corea del Nord. Secondo l'FBI (2020) il gruppo è stato responsabile di diversi attacchi informatici, inclusi il furto di oltre 81 milioni di dollari dalla banca centrale del Bangladesh nel 2016 e attacchi a banche, casinò, istituzioni governative e aziende private in tutto il mondo. L'obiettivo principale del gruppo

sembra essere il finanziamento del regime nordcoreano attraverso il furto di denaro da banche e istituzioni finanziarie estere, e le sue attività sembrano essere controllate dal governo nordcoreano.

Organizzazioni criminali (*cyber*)

Le organizzazioni criminali, come la mafia e le bande criminali, hanno iniziato a interessarsi sempre di più alle attività illecite online, come la truffa e il furto di identità, a causa della grande quantità di denaro che possono guadagnare in questo modo. Secondo il rapporto della Commissione Europea (2017) sulle attività criminali online, le organizzazioni criminali utilizzano Internet per attività come le frodi bancarie, le estorsioni, la diffusione di malware e le truffa legate alle carte di credito.

Le organizzazioni criminali spesso operano in modo organizzato e professionale, utilizzando le tecniche più avanzate per infiltrarsi nei sistemi delle vittime e rubare informazioni o denaro. Spesso lavorano in gruppi, suddividendo le mansioni per massimizzare l'efficienza e la sicurezza delle loro attività.

Secondo un rapporto dell'Europol (2021), le organizzazioni criminali hanno mostrato una crescente capacità di adattamento e di utilizzo delle nuove tecnologie per condurre le loro attività illegali, come l'utilizzo di criptovalute per effettuare transazioni finanziarie anonime.

Le organizzazioni criminali hanno come obiettivo principale il profitto, e utilizzano le attività criminali online per aumentare i loro guadagni. Al contempo, il loro coinvolgimento in attività illegali online può anche rappresentare una minaccia per la sicurezza nazionale e internazionale.

Tuttavia, secondo Lusthaus (2013) citato in Salini (2023), non è possibile paragonare il crimine organizzato tradizionale alle organizzazioni criminali *cyber* per via

delle differenze nell'organizzazione gerarchica e nelle relazioni interpersonali con gli individui che li compongono.

I gruppi più famosi sono REvil e Lockbit 2.0. REvil è un gruppo di cybercriminali attivo dal 2019, noto per i suoi attacchi ransomware. Nonostante sia stato smantellato verso la fine del 2021 grazie ad un'operazione congiunta tra Stati Uniti e Unione Europea, i segni di un possibile ritorno sono apparsi nell'aprile 2022.

Lockbit 2.0 è un'altra *cyber gang* che ha colpito diverse aziende in vari paesi, tra cui Regno Unito, Cile, Taiwan e Italia. Caratteristica del gruppo è la pubblicazione di un conto alla rovescia per il pagamento del riscatto sul *dark web*, accompagnato dalla minaccia di divulgare i dati rubati (F3RM1, 2022).

Cyber-mercenari

I cyber-mercenari sono gruppi di *hacker* professionisti (o esperti di sicurezza informatica) che forniscono servizi di *hacking* a pagamento (operazioni offensive) a governi, organizzazioni militari, agenzie di intelligence o aziende private o individui che vogliono raggiungere obiettivi specifici.

Secondo un rapporto del *Council on Foreign Relations*, questi gruppi hanno una crescente influenza sulla sicurezza informatica globale e hanno svolto un ruolo nella crisi in Ucraina del 2015[17].

I cyber-mercenari utilizzano tecniche di hacking avanzate per ottenere l'accesso ai sistemi o per distruggere informazioni. Possono essere assunti da governi o aziende per condurre operazioni offensive, il che significa che possono agire con l'autorizzazione e le risorse del loro committente. Inoltre, possono operare in modo molto discreto e difficile da rilevare.

Secondo il rapporto dell'ENISA (Lella et al., 2022) sull'evoluzione delle minacce informatiche, i cyber-mercenari possono essere impiegati anche per attaccare concorrenti commerciali o per rubare proprietà intellettuale. Inoltre, possono

[17] Cyber Mercenaries and the Crisis in Ukraine, January 30, 2018. 4:11 pm (EST), https://www.cfr.org/blog/cyber-mercenaries-and-crisis-ukraine

essere ingaggiati per condurre attacchi di tipo politico o per sabotare le infrastrutture critiche di un paese.
Il loro scopo principale è quello di condurre operazioni di spionaggio e attacchi informatici mirati contro obiettivi di interesse nazionale o strategico ottenendo così informazioni o accesso a sistemi protetti, senza essere rilevati. Inoltre, possono essere impegnati anche in operazioni di sabotaggio, come la distruzione dei sistemi IT di un'organizzazione, la manipolazione di dati sensibili o l'interruzione dei servizi.

In generale, i cyber-mercenari sono molto ben finanziati e hanno accesso a strumenti e risorse avanzate, il che rende difficile contrastarli. Tuttavia, il loro operato può essere limitato attraverso la cooperazione internazionale e il rafforzamento della sicurezza informatica delle organizzazioni e delle infrastrutture critiche.

Competitor hacker

Questi sono gruppi che agiscono per il proprio interesse economico o politico, ad esempio per danneggiare un concorrente o per rubare informazioni proprietarie.
Essi sono anche noti come gruppi di intelligence economica o *"Competitor Intelligence Professionals" o "Intelligence Champions"* (Martre, 1994).
Secondo un rapporto di ENISA (2020) sullo spionaggio cibernetico, i competitor cercano di ottenere informazioni su prodotti, strategie di *marketing*, proprietà intellettuale e piani di espansione dell'azienda concorrente. Il rapporto afferma che questi gruppi operano spesso per conto di aziende che cercano di acquisire informazioni sui loro concorrenti o di sabotare le loro attività.
I competitor sono gruppi che cercano di ottenere un vantaggio competitivo di mercato danneggiando le attività delle loro concorrenti, ad esempio rubando informazioni riservate o mettendo fuori uso i sistemi informatici avversari. Inoltre, possono utilizzare tecniche di spionaggio industriale per carpire i segreti commerciali dei propri avversari.

Secondo il rapporto sulla sicurezza informatica di Reuters (2014), questi gruppi spesso si concentrano su specifici obiettivi come i sistemi di produzione o i dati della proprietà intellettuale, utilizzando spesso metodi sofisticati come il spear-phishing e il malware personalizzato. Spesso sono altamente motivati dalla concorrenza commerciale e possono sfruttare tecniche di *hacking* sofisticate (tra questi vi sono l'uso di *spyware*, social media intelligence, vulnerabilità informatiche) al fine di poter accedere ai sistemi informatici delle aziende rivali o utilizzare tecniche di ingegneria sociale per raccogliere informazioni sensibili.
L'obiettivo finale dei competitor è acquisire un vantaggio competitivo sul mercato e influenzare le decisioni dei concorrenti.

Hacker tradizionali:
Questi sono individui o gruppi che agiscono per il proprio divertimento o per dimostrare le proprie abilità tecniche. Secondo il rapporto di Verizon (2022) sulle minacce informatiche, questi hacker spesso cercano di accedere a sistemi vulnerabili per testare le loro abilità. Sono motivati principalmente dalla curiosità tecnica o dall'orgoglio personale.
Secondo uno studio del 2020 della società di consulenza Infosys (Duncan, 2020), gli hacker tradizionali sono spesso motivati da obiettivi finanziari, politici o di spionaggio. Questi attori possono agire come singoli individui o come membri di gruppi di hacker. Il loro obiettivo principale è spesso quello di violare la sicurezza informatica al fine di ottenere informazioni sensibili o danneggiare il sistema informatico del "target".
Gli hacker tradizionali possono utilizzare una varietà di tecniche per violare la sicurezza informatica, come ad esempio l'ingegneria sociale, l'utilizzo di *software* malevolo o la forza bruta. Le conseguenze delle loro azioni possono comportare, ad esempio, il furto di dati sensibili, danni alla reputazione dell'organizzazione colpita o persino l'interruzione delle operazioni aziendali.

Hacktivisti

Gli hacktivisti sono individui o gruppi di *hacker* che utilizzano le loro abilità tecniche per scopi politici o sociali. Questi gruppi sono solitamente composti da attivisti, *hacker* etici ed esperti di sicurezza informatica che utilizzano le loro competenze per portare avanti un messaggio politico o sociale, utilizzando spesso internet come mezzo per farlo.

Gli obiettivi degli hacktivisti possono essere molteplici (Jordan et al. 2014): ad esempio, possono mirare a sostenere una causa sociale o politica, a denunciare un'ingiustizia o una violazione dei diritti umani, o ancora a far emergere la verità su una vicenda controversa. In molti casi, gli hacktivisti cercano di diffondere il loro messaggio attraverso l'attacco di siti web o il furto di informazioni sensibili, come ad esempio quelli delle istituzioni governative o delle aziende.

Un esempio di hacktivismo è rappresentato dal gruppo *Anonymous* (Coleman, 2014), noto per aver portato avanti numerose azioni di protesta e attivismo online contro governi e organizzazioni considerate antidemocratiche o corrotte.

Terroristi

I gruppi terroristici che utilizzano la tecnologia informatica per scopi distruttivi sono un fenomeno relativamente nuovo, ma sempre più diffuso (Chen et al. 2014). Essi sono solitamente caratterizzati dall'uso di Internet per comunicare, coordinarsi e diffondere la loro propaganda, ma possono anche utilizzare tecniche di *cyberwarfare* per attaccare obiettivi governativi o civili.

Gli obiettivi dei gruppi terroristici possono variare notevolmente a seconda del loro ideale politico o religioso. Tuttavia, molti di questi gruppi cercano di destabilizzare i governi, causare panico e diffondere la loro propaganda attraverso la diffusione di messaggi o la divulgazione di immagini di attacchi.

Estorsori

Si tratta in questo caso di gruppi che cercano di ottenere un guadagno finanziario attraverso l'estorsione, ad esempio mediante il blocco di sistemi informatici con

ransomware o attraverso la minaccia di divulgare informazioni riservate. Secondo la società NordVPN [18] (2022), i gruppi di estorsione utilizzano spesso metodi come il *phishing*, il *malware* e la forza bruta per ottenere l'accesso ai sistemi delle loro vittime.

I "*ransomware attacker*" sono spesso altamente motivati dal denaro e possono essere molto aggressivi nelle loro richieste di riscatto. Possono utilizzare metodi sofisticati di crittografia per bloccare i sistemi della loro vittima e impedire l'accesso ai dati. Inoltre, possono cercare di mascherare la loro identità utilizzando tecnologie come la rete TOR o la crittografia *end-to-end*. Gli estorsori utilizzano minacce o attacchi informatici per carpire denaro o informazioni sensibili alle loro vittime. Di solito, chiedono il pagamento di un riscatto per sbloccare l'accesso ai dati crittografati o per evitare la divulgazione di informazioni compromettenti. Spesso utilizzano tecniche di *ransomware* e di DDoS (RDoS) combinate per esercitare pressioni sulle loro vittime (Check Point, 2022).

Uno dei gruppi più attivi e specializzati in attacchi ransomware è il gruppo Conti. Attivo dal 2017 è un'organizzazione russofona altamente strutturata, con oltre 100 membri, ed è nota per la sua spietatezza per aver attaccato istituzioni sanitarie durante la pandemia (F3RM1, 2022). È uno dei promotori del cosiddetto RaaS[19], ovvero la predisposizione e fornitura della piattaforma di attacco dietro corrispettivo in criptovalute da parte dei clienti (Salini, 2023).

Insider

Questi sono individui all'interno di un'organizzazione che abusano della loro autorizzazione per accedere a informazioni o sistemi a cui non dovrebbero avere accesso.

Gli insider sono individui che lavorano all'interno di un'organizzazione e hanno accesso privilegiato alle risorse informatiche e ai dati dell'azienda.

[18] *What is cyber extortion*? https://nordvpn.com/blog/cyberextortion/
[19] RaaS: Ransomware as a Service

Secondo il rapporto sulla sicurezza informatica di Verizon (2022), gli *insider* possono essere motivati da una varietà di fattori, tra cui la vendetta, il guadagno finanziario o l'orgoglio personale.

Inoltre, potrebbero causare danni significativi all'organizzazione per via dell'elevato accesso a dati e sistemi aziendali che, grazie anche allo sfruttamento delle proprie credenziali di accesso, li rendono di difficile individuazione.

Gli obiettivi degli insider possono essere molteplici, come rubare proprietà intellettuale, informazioni sensibili dell'azienda o sabotare le operazioni dell'organizzazione.

Secondo il rapporto DBIR del 2020 di Verizon, il 30% degli attacchi informatici che coinvolgono insider è motivato da motivi finanziari, mentre il 23% è causato da motivi personali, come vendetta o atti vandalici. Altri obiettivi possono includere il furto di informazioni personali o la compromissione della sicurezza dell'azienda per ragioni politiche o sociali.

CAPITOLO 4 – LE DIFESE

Le attività di difesa e di prevenzione sono essenziali per la protezione degli *asset* dalla minaccia cibernetica. Queste consistono in una serie di misure di sicurezza di varia natura, tra le quali: la protezione degli endpoint, la gestione degli accessi, la crittografia dei dati, il monitoraggio della rete e la gestione degli incidenti, che vengono adottate per proteggere le infrastrutture IT.
Inoltre, la difesa del ciberspazio richiede anche la collaborazione con altre organizzazioni e autorità, come le forze dell'ordine e le agenzie di *intelligence*, per garantire una risposta efficace alle minacce cibernetiche e una cooperazione in caso di attacchi informatici di portata nazionale o internazionale.

Finora sono state analizzate le peculiarità inerenti agli scenari della *Cyber Warfare*, alle tipologie di minacce, alle principali metodologie di attacchi, agli attori che agiscono nel ciberspazio.
Nel mondo odierno, poiché le minacce cibernetiche sono ormai una realtà costante, consolidata e continuativa, richiedono una serie di strategie di difesa robuste e misure preventive per mantenere sicuri i nostri sistemi digitali. Queste metodologie includono una serie di tattiche, tecniche e procedure (TTP), così come l'uso di tecnologie avanzate.

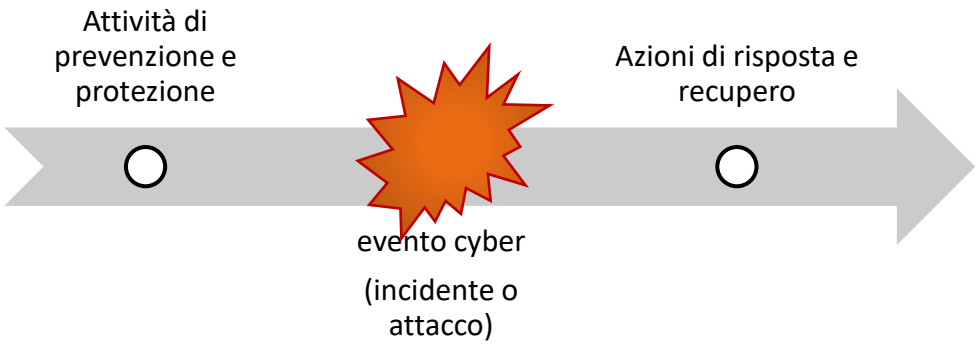
La sicurezza informatica e in particolare la difesa cibernetica hanno sempre viaggiato di pari passo con gli elementi descritti sopra.
Inoltre, le azioni di difesa possono avere una natura proattiva o reattiva. Infatti, a seconda della prospettiva, a monte o a valle di un evento, è possibile parlare di azioni di prevenzione/protezione e azioni di risposta/recupero (tabella 6).

- **Prevenzione / Protezione**: Questa fase include l'implementazione di misure proattive per evitare gli attacchi informatici. Questo può includere la

formazione del personale, l'installazione di *software antivirus*, l'implementazione di *firewall*, l'uso di autenticazione a due fattori, e così via.

- **Risposta / Recupero**: Questa fase viene dopo che un incidente si è verificato. Include attività come l'identificazione dell'incidente, l'analisi dell'impatto, l'implementazione di misure per limitare i danni, la risoluzione del problema e il ripristino dei sistemi al normale funzionamento. Questa fase può anche includere un'analisi post-incidente per apprendere dall'incidente e migliorare le misure di sicurezza per il futuro.

Tabella 6 - Timeline di un evento e azioni connesse



Questi termini fanno parte di un modello di sicurezza informatica più ampio noto come ciclo di gestione degli incidenti (Cichonski et al., 2012), che può essere suddiviso in diverse fasi:

1. **Preparazione**: Questa fase riguarda l'istituzione di un team di risposta agli incidenti, la creazione di piani e procedure di risposta agli incidenti, la formazione del personale e l'installazione e la configurazione delle tecnologie di rilevamento e prevenzione degli incidenti.
2. **Identificazione**: Questa fase riguarda la scoperta di un incidente potenziale, che può essere identificato attraverso i sistemi di rilevamento degli incidenti, i rapporti degli utenti o l'analisi dei dati di rete.
3. **Contenimento**: Una volta identificato un incidente, è importante contenerlo per prevenire ulteriori danni. Questo può includere la disconnessione

dei sistemi infetti dalla rete, l'isolamento delle aree di rete compromesse o l'implementazione di regole di blocco del *firewall*.

4. **Eliminazione**: In questa fase, l'obiettivo è eliminare la causa dell'incidente, che potrebbe includere la rimozione del *malware*, la correzione delle vulnerabilità sfruttate o l'aggiornamento dei software compromessi.
5. **Recupero**: Dopo che la causa dell'incidente è stata eliminata, i sistemi possono essere riportati alla normalità. Ciò può includere il ripristino dei dati da backup, la verifica dell'integrità dei sistemi e il monitoraggio per garantire che l'incidente sia stato completamente risolto.
6. **Apprendimento / Lesson Learned**: Dopo la risoluzione di un incidente, è importante esaminare l'accaduto per capire cosa è andato storto e come prevenire simili eventi in futuro. Questo può includere l'analisi delle cause scatenanti, l'aggiornamento delle politiche e delle procedure e la formazione del personale sulla base delle lezioni apprese.

Secondo Franchina (2018) le contromisure possono essere suddivise in tre grandi macroaree (fisiche, informatiche e procedurali) e possono anche essere raggruppate in 10 categorie:

1. Identificazione e autenticazione (con *password*, *pin*, impronta digitale e biometria)
2. Controllo accessi (individuazione delle modalità di accesso non autorizzato)
3. Registrazione degli eventi (all'interno di un SOC)
4. Audit (verifiche periodiche e continuative)
5. Analisi delle vulnerabilità (Penetration test e scansione delle vulnerabilità)
6. Mantenimento della continuità operativa (*contingency plan, disaster recovery* e *backup*)
7. Istituzione di corsi di formazione (*security awareness*)
8. E-mail e internet (monitoraggio)
9. Definizione di alcuni aspetti tecnici di difesa attiva (e.g. *antivirus* e *firewall*) e prevenzione delle intrusioni (IDS)

10. Ruolo dei log (di sicurezza, dei *software* anti *malware*, di accesso remoto, dei *web proxy* e dei *router*)

Una tecnica di analisi strutturata che potrebbe legarsi alle tre macroaree indicate sopra è il modello S.H.E.L.L. qui rappresentato nella figura sottostante (Hawkins & Orlady, 1993).

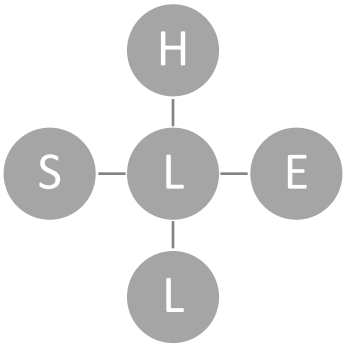


Figura 10 - Il modello S.H.E.L.L per l'analisi degli incidenti organizzativi

Sviluppato originariamente dall'aviazione, è un modello di analisi degli incidenti che prende in considerazione i diversi fattori che possono contribuire a un incidente.
Il modello è un acronimo per *Software* (S), *Hardware* (H), *Environment* (E), *Liveware* (L) e *Liveware-Interface* (L).

Questo modello può essere applicato alla difesa cibernetica nel seguente modo:

- ***Software*** (**S**): Questo rappresenta i programmi, i sistemi operativi e gli altri software utilizzati in un'organizzazione. Nel contesto della difesa, l'analisi del software può includere la verifica della presenza di vulnerabilità note, l'efficacia dei programmi antivirus o di altre misure di sicurezza del software e la presenza di software non autorizzato o malevolo.
- ***Hardware*** (**H**): Rappresenta *l'hardware* fisico utilizzato, come *server*, *computer*, *router* e altri dispositivi di rete. L'analisi *dell'hardware* può

includere la verifica della sicurezza fisica dei dispositivi, la presenza di dispositivi non autorizzati e l'efficacia delle misure di sicurezza *dell'hardware*, come i *firewall hardware*.

- ***Environment*** (**E**): Rappresenta l'ambiente in cui *l'hardware* e il *software* operano. In questo ambito, l'ambiente può includere il contesto di rete, le condizioni fisiche (come la sicurezza dei locali), le condizioni operative e le minacce esterne, come i tentativi di attacco cibernetico.
- ***Liveware*** (**L**): Ovvero le persone coinvolte, come gli utenti, gli amministratori di sistema e i responsabili della sicurezza. L'analisi del "*liveware*" può includere l'efficacia della formazione sulla sicurezza, la consapevolezza delle minacce, la conformità alle politiche di sicurezza e altri fattori umani.
- ***Liveware-Interface*** (**L-L**): Infine, le interazioni tra le persone e gli altri componenti del sistema. Nel contesto della *cyber defense*, l'analisi del "*liveware-interface*" può includere la facilità d'uso dei sistemi di sicurezza, la chiarezza delle politiche e delle procedure di sicurezza, e l'efficacia delle comunicazioni sulla sicurezza.

Entrando più nello specifico, vi sono delle componenti fondamentali nella difesa cibernetica. Tra queste possiamo annoverare le principali:

S - H	• La **gestione degli accessi**, che comporta il controllo di chi può accedere a quali risorse in un sistema o una rete (Cisco, 2023). Questo può includere l'uso di privilegi minimi, dove agli utenti viene dato solo l'accesso di cui hanno bisogno per svolgere i loro compiti, e l'isolamento di sistemi sensibili o critici. • La **sicurezza dei dati** è un altro aspetto cruciale, che si concentra sulla protezione dei dati da accessi non autorizzati o da manipolazioni. Questo può includere l'uso di *backup* regolari, la

	protezione contro malware come ransomware e l'uso di sistemi di prevenzione delle perdite di dati (DLP) (Lee et al. 2017). • Il **rilevamento delle intrusioni** è un altro strumento importante nella difesa cibernetica. I sistemi di rilevamento delle intrusioni (IDS) monitorano le reti alla ricerca di attività sospette o anomale, permettendo ai responsabili della sicurezza di rispondere rapidamente a possibili attacchi (ENISA, 2016). • **L'autenticazione *multi-factor* (MFA)** fornisce un ulteriore strato di sicurezza, richiedendo agli utenti di fornire più di un tipo di credenziale per accedere a un sistema. Questo può includere qualcosa che l'utente sa (come una *password*), qualcosa che l'utente ha (come una *smart card*) e qualcosa che l'utente è (come un'impronta digitale) (Moses et al., 2016). • La **crittografia anamorfica** è un altro strumento fondamentale per la sicurezza cibernetica, utilizzato per proteggere i dati in transito e a riposo. La crittografia rende i dati inintelligibili senza la chiave di crittografia corretta, proteggendo i dati da accessi non autorizzati anche se vengono intercettati (NIST, 2020). • La **virtualizzazione** e il **sandboxing** possono essere utilizzate per isolare le applicazioni o i sistemi potenzialmente insicuri, impedendo loro di danneggiare il resto del sistema (VMware, 2019).
H	• Soluzioni di sicurezza **Firewall** (Ding, 2020). • **Sistemi di monitoraggio** dei tentativi di accesso sospetti (Steingartner, 2021). • Adozione di **filtri *antispam*.** • **Gestione delle vulnerabilità**: Questo processo comporta l'identificazione, la classificazione, la risoluzione e il

	mitigamento delle vulnerabilità nei sistemi informatici. Ciò può includere l'utilizzo di *software* di scansione delle vulnerabilità e l'implementazione di patch di sicurezza (Mell, 2005). • **Piani di risposta agli incidenti**: Questi piani delineano le procedure da seguire in caso di un attacco informatico. Possono includere procedure di *escalation*, comunicazione interna ed esterna, e piani di ripristino (National Institute of Standards and Technology, 2012).
S	• Procedure di **gestione e identificazione delle vulnerabilità e degli incidenti** (Smith, 2020). • **Politiche di sicurezza solide**: Le organizzazioni dovrebbero avere politiche chiare e rigorose per la gestione delle informazioni riservate. Ciò può includere procedure per la condivisione delle credenziali di accesso, il trattamento delle informazioni riservate e il rapporto con i clienti e i fornitori (Stallings & Brown, 2012). • È importante verificare periodicamente la **conformità** alle politiche di sicurezza e testare la consapevolezza del personale sui rischi di social engineering attraverso esercizi di *phishing* simulati o altre valutazioni (Mitnick & Simon, 2002).
E	• Applicazione di **linee guida** e di **best practice** di matrice istituzionale (ENISA, 2016) • Applicazione di **norme**, **direttive** e **regolamenti** per la creazione di un *framework* di sicurezza, riduzione del rischio, promozione della responsabilità, garantire la continuità operativa.
L	• **Formazione e consapevolezza del personale**: La formazione del personale sulle tecniche di *social engineering* è una delle difese più efficaci. Gli utenti devono essere in grado di

	riconoscere e rispondere adeguatamente a tentativi di *phishing*, pretesti e altre tecniche di ingegneria sociale (Hadnagy, 2010). • Aumentare la **consapevolezza** sul mondo della *Cyber Warfare* e degli attacchi cibernetici attraverso la formazione del personale può aiutare a prevenire gli attacchi e ridurre il rischio. Questo può includere formazione su come riconoscere e rispondere alle e-mail di *phishing*, sull'importanza di manutenzione del *software* mediante gli aggiornamenti che possono risolvere le vulnerabilità, la gestione sicura dei dati sensibili (Brodie, 2009).

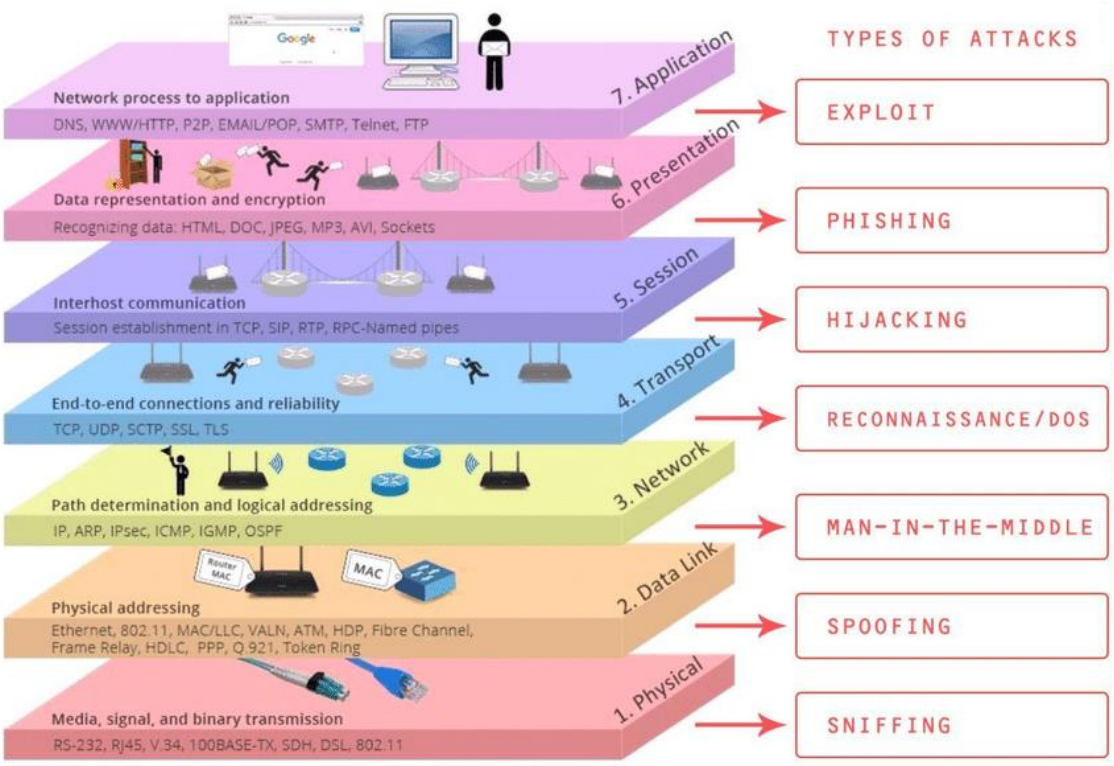


Figura 11 - Information Systems' Open Systems Interconnection Model (OSI-Model) layers and types of attack mapping © 2021 Steingartner

Il modello illustrato in figura 11 invece rappresenta un approccio olistico alla sicurezza informatica che può essere applicato sia alla prevenzione degli attacchi, sia alla risposta e al recupero quando gli attacchi si verificano.

Questo mette in relazione i livelli OSI con le modalità possibili di attacco. Quindi si tratta di un modello di analisi preventiva che può contemplare le forme di ragionamento deduttivo, induttivo e abduttivo indicate da Moore (2007), citato in Conio (2018), per poter studiare le tipologie di attacco in relazione al singolo livello OSI preso in considerazione o viceversa.

Per prevenire gli attacchi informatici prima che si verifichino, è fondamentale una robusta difesa contro le minacce. Questa può essere realizzata attraverso un approccio che combina diverse soluzioni di sicurezza o attraverso l'impiego di un'intelligenza avanzata sulle minacce, distribuita in tutto l'ecosistema di sicurezza (Steingartner, 2021). Come si evince in figura 11, esistono vari tipi di attacchi informatici che possono essere correlati a ogni livello del Modello di Interconnessione dei Sistemi Aperti (OSI-Model), sviluppato dall'Organizzazione Internazionale per la Standardizzazione (ISO).

Il modello OSI è noto per la sua capacità di standardizzare le funzioni di comunicazione di un sistema informatico e di comunicazione, indipendentemente dalla tecnologia sottostante e dalla struttura interna. L'obiettivo del modello è di garantire la compatibilità tra diversi sistemi di comunicazione attraverso l'uso di protocolli di comunicazione standardizzati. Inoltre, i protocolli di sicurezza rivestono un ruolo cruciale e irrinunciabile in questo contesto.

Riprendendo quanto analizzato nel capitolo 2 circa le fasi della *Attack Chain Analysis* e secondo quanto visto col modello OSI e l'applicazione del pensiero critico, Hutchins et al. (2011) hanno applicato al modello una serie di metodologie di difesa, ipotizzando così una matrice utile a determinare gli aspetti difensivi.

La tabella sottostante (tabella 7) descrive una matrice di azioni di sicurezza informatica basata sulla dottrina del Dipartimento della Difesa degli Stati Uniti (2011). Questa tabella mostra come vari strumenti, tra cui sistemi di rilevamento delle intrusioni, patch di sicurezza e tecniche di prevenzione, possono essere

utilizzati per contrastare gli attacchi informatici. La matrice evidenzia l'importanza sia di metodi tradizionali come i sistemi di rilevamento delle intrusioni di rete e le liste di controllo del firewall, sia di pratiche come la registrazione degli audit e la vigilanza degli utenti nel rilevare attività sospette.

Tabella 7 – Rielaborazione di "Course of action Matrix" (U.S. DoD, 2006) in Hutchins et al. (2011).

Phase	**Detect**	**Deny**	**Disrupt**	**Degrade**	**Deceive**	**Destroy**
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honetpot	

Infine, in un mondo sempre più connesso, possiamo definire alcuni aspetti legati alla protezione dei sistemi di Tecnologia Operativa (OT) e di come questo possa farci comprendere l'importanza di un apporto olistico alla difesa cibernetica. Ecco alcuni approcci proposti da Stouffer et al. (2015) nel report realizzato dal NIST e dal SANS Institute (2016):

1. **Identificazione e valutazione dei rischi**: È essenziale identificare e valutare i rischi che potrebbero minacciare la sicurezza dei sistemi OT.
2. **Segmentazione di rete**: La segmentazione di rete è un metodo efficace per separare i sistemi OT dalle reti IT, riducendo la possibilità che un attacco alla rete IT possa compromettere la rete OT.
3. **Aggiornamenti regolari**: Mantenere i *software* e i *firmware* aggiornati è fondamentale per proteggere contro le vulnerabilità note. Tuttavia, è importante notare che gli aggiornamenti possono essere più difficili da

implementare in un ambiente OT rispetto a un ambiente IT a causa delle esigenze di *uptime* e stabilità.

4. **Monitoraggio e rilevamento delle intrusioni:** Strumenti di monitoraggio e rilevamento delle intrusioni possono aiutare a identificare rapidamente eventuali attività sospette o non autorizzate.
5. **Piani di risposta agli incidenti**: Avere un piano di risposta agli incidenti può aiutare a minimizzare il danno di un attacco informatico.
6. **Formazione e consapevolezza del personale**: Il personale che lavora con i sistemi OT dovrebbe ricevere una formazione adeguata sulla sicurezza informatica, compresi i tipi di minacce, come riconoscerle e come rispondere.
7. ***Backup* regolari**: I *backup* regolari dei sistemi OT possono garantire che i dati possano essere ripristinati rapidamente in caso di attacco.
8. **Controllo degli accessi**: Limitare l'accesso ai sistemi OT solo a personale autorizzato può aiutare a prevenire e rilevare attività non autorizzate.

Gli aspetti citati sopra sono altrettanto validi anche negli ambiti non OT e in aggiunta potremmo aggiungere anche i seguenti aspetti da non trascurare:

- Utilizzare *password* sicure e modificarle in modo regolare.
- Compartimentare l'accesso alle informazioni e ai sistemi sensibili solo a chi è realmente preposto alla funzione.
- Condurre regolarmente test di sicurezza e di penetrazione.
- Analizzare gli avvisi di sicurezza, bollettini e note CVE, ovvero gli strumenti che aiutano a identificare le vulnerabilità, gli aspetti di sicurezza e gli exploit relativi a un sistema informatico.
- Analizzare i rapporti di *Cyber Threat Intelligence* (CTI) che descrivono tattiche, tecniche e procedure (TTP), tipologie di attori e di sistemi presi di mira e altre informazioni relative alle minacce forniscono maggiore consapevolezza situazionale a un'organizzazione.

In conclusione, le minacce informatiche si presentano in molte forme e possono risultare estremamente difficili da prevenire. La loro prevenzione rappresenta quindi una sfida.

Tuttavia, comprendendo i tipi di minacce esistenti e seguendo le migliori pratiche per la sicurezza, le organizzazioni e gli individui possono ridurre il rischio di cadere vittime di un attacco informatico.

Rimane fondamentale mantenere un aggiornamento costante riguardo le ultime evoluzioni nel campo della sicurezza informatica e adattare le proprie misure di protezione di conseguenza.

CAPITOLO 5 – SFIDE E PROSPETTIVE FUTURE

Mentre la tecnologia continua a evolversi, lo fanno anche le minacce che presenta. Le sfide future per la sicurezza informatica derivano dall'evoluzione stessa delle tecnologie e dei metodi di attacco. Per rimanere al passo, le difese devono anticipare e prepararsi per le possibili evoluzioni future degli attacchi informatici.

L'ENISA (2023), che tra i propri obiettivi prevede il miglioramento della resilienza della sicurezza informatica dell'UE, l'aumento della consapevolezza delle minacce future e la promozione delle contromisure tra gli Stati membri dell'UE e le parti interessate, nel corso del 2022 ha identificato le 10 principali minacce emergenti alla sicurezza informatica che si prevede si verificheranno entro il 2030 (figura 12). Tra queste troviamo:

1. Compromissione di una catena di approvvigionamento (*supply chain attack*) aziendale
2. Campagne di disinformazione avanzata
3. Aumento dell'autoritarismo della sorveglianza digitale / perdita della privacy
4. Errore umano e sistemi *legacy* [20]sfruttati all'interno di ecosistemi cibernetici-fisici
5. Attacchi mirati potenziati dai dati dei dispositivi intelligenti
6. Mancanza di analisi e controllo dell'infrastruttura e degli oggetti spaziali
7. Aumento delle minacce ibride avanzate
8. Scarsità di competenze
9. Fornitori di servizi ICT transfrontalieri come unico punto di fallimento
10. Abuso dell'intelligenza artificiale

[20] sono sistemi informatici o software obsoleti o superati che sono ancora in uso nonostante l'introduzione di tecnologie più recenti. Questi sistemi possono essere costosi da mantenere e aggiornare e possono rappresentare rischi di sicurezza e compatibilità con le nuove tecnologie

Il gruppo di esperti di prospettiva dell'ENISA, la rete dei CSIRT e gli esperti CyCLONe [21]dell'UE hanno condotto un esercizio di simulazione nel quale hanno utilizzato una varietà di tecniche di analisi strutturata, tra cui l'analisi PESTLE[22], il *Threatcasting* e la prototipazione SFP[23], per identificare le minacce e definire le priorità.

L'esercitazione ha quindi incluso l'esplorazione e l'analisi collaborativa di fattori politici, economici, sociali e tecnologici. Grazie alla metodologia SFP ovvero alla possibilità, attraverso la narrazione, di esplorare una varietà di futuri affrontati da diverse angolazioni.

La metodologia di *Threatcasting* invece attinge dai tradizionali studi sul futuro e dal pensiero strategico militare. L'idea consisteva nel dedurre modelli di ambienti futuri utilizzando la ricerca. L'analisi ha quindi incluso tecniche di pianificazione degli scenari e sono stati ideati 5 scenari:

1. *Blockchain*, *deepfake* e criminalità informatica in un ambiente ricco di dati;
2. Città intelligenti ecologiche, sostenibili e interconnesse (attori non statali);
3. Più dati, meno controllo;
4. Energia sostenibile, forza lavoro automatizzata/a breve termine;
5. Legislazione, pregiudizi, estinzioni e minacce globali.

Le minacce identificate includono la compromissione della catena di approvvigionamento delle dipendenze del *software*, campagne di disinformazione avanzate, aumento dell'autoritarismo della sorveglianza digitale/perdita di *privacy*, errore umano e sistemi *legacy* sfruttati all'interno di ecosistemi cyber-fisici, attacchi mirati potenziati dai dati dei dispositivi intelligenti, mancanza di analisi e controllo di infrastrutture e oggetti spaziali, aumento di minacce ibride avanzate,

[21] Progetto UE-CyClONe: Cybersecurity Competence for Research and Innovation https://www.consilium.europa.eu/it/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/

[22] Fattori politici, economici, sociali, tecnologici, ambientali e legali

[23] SFP si basa su uno scenario futuro derivato dalle tendenze e vissuto dal punto di vista di un personaggio immaginario.

carenza di competenze, fornitori di servizi TLC transfrontalieri come singolo punto di errore e abuso di intelligenza artificiale.

Le conclusioni dell'esercizio di simulazione intendono servire da incentivo ad agire per migliorare la resilienza della cybersicurezza dell'UE.

Il gruppo di lavoro degli Stati membri dell'UE all'ENISA ha quindi fornito l'opportunità di discutere la gestione delle crisi informatiche, la direttiva NIS2 e la certificazione.

Figura 12 © 2023 ENISA - Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride! https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030

Intelligenza Artificiale e Apprendimento Automatico

L'intelligenza artificiale (AI[24]) e l'apprendimento automatico (ML[25]) stanno diventando sempre più importanti nella *cybersecurity*, sia per la difesa che per

[24] *Artificial Intelligence*
[25] *Machine Learning*

l'attacco. Gli attaccanti possono utilizzare l'AI e il ML per automatizzare gli attacchi, rendendoli più veloci ed efficaci. Ad esempio, possono utilizzare l'AI per condurre attacchi di *phishing* più convincenti o per trovare rapidamente vulnerabilità nei sistemi di sicurezza (Brundage et al., 2018).

l'AI è diventata un'arma per la cybercriminalità, che la utilizza per effettuare attacchi più rapidi e precisi. Gli hacker possono sfruttare l'AI per individuare vulnerabilità nei sistemi IT, generare e-mail di phishing più realistiche, o introdurre dati malevoli nei set di dati di apprendimento. Inoltre, con l'avvento dei motori GPT[26], un tipo di modello di apprendimento automatico utilizzato per generare testo, i cybercriminali potrebbero utilizzare questa architettura per generare testi efficaci che, se usati in modo inappropriato, potrebbero alimentare attività malevoli come il *phishing* o lo *spear phishing*. Il *software* può infatti generare email che sembrano legittime, come richieste di bonus o aggiornamenti software urgenti, rendendo più efficaci le truffe online (F3RM1, 2023).

Nonostante questi rischi, l'AI può anche svolgere un ruolo fondamentale nella difesa contro gli attacchi informatici. Le intelligenze artificiali possono rilevare le attività criminali più accuratamente rispetto ai sistemi tradizionali, e possono aiutare i *team* di sicurezza informatica a individuare anomalie e criticità nel flusso dei dati più rapidamente e con maggiore precisione.

In definitiva presenta sia rischi che opportunità. Nonostante le sfide, l'uso intelligente dell'AI può aiutare a prevenire minacce e a progettare strategie di difesa più efficaci (F3rm1 Foundation, 2022).

Internet delle Cose (IoT – *Internet of Things*)

L'Internet delle Cose (IoT) rappresenta un'altra sfida significativa per la sicurezza informatica. Molti dispositivi IoT sono noti per le loro scarse misure di sicurezza, rendendoli bersagli facili per gli *hacker*. Questi dispositivi possono poi essere utilizzati per condurre attacchi DDoS o per accedere a reti protette (Kolias et al.,

[26] GPT: Generative Pretrained Transformer

2017). Nel campo delle IC, possiamo trovare le componenti fondamentali quali: BMS, SCADA, PCL, HMI, RTU, DCS.

Attacchi alla catena di fornitura (*supply chain*)

Gli attacchi alla catena di fornitura sono un'altra minaccia emergente. Gli attacchi come quello a SolarWinds dimostrano come gli *hacker* possono infiltrarsi nelle reti compromettendo i fornitori di *software* o *hardware* (Perlroth, 2021). Questo tipo di attacco può avere un impatto significativo, poiché può permettere agli attaccanti di accedere a molte organizzazioni attraverso un unico punto di ingresso.

Governance

La relazione del DIS sottolinea l'importanza della collaborazione internazionale per garantire la sicurezza cibernetica a livello globale. In particolare, viene evidenziata la necessità di sviluppare norme e standard internazionali sulla sicurezza cibernetica e di promuovere la cooperazione tra gli Stati per contrastare le minacce cibernetiche transnazionali.

Per affrontare la minaccia della *Cyber Warfare,* è fondamentale adottare una gestione integrata dei rischi, come sottolineato dalla relazione annuale del DIS del 2022. Questo significa implementare misure di sicurezza informatica a livello organizzativo, tecnico e umano, nonché cooperare a livello nazionale e internazionale per contrastare le minacce cibernetiche. Inoltre, la relazione del DIS sottolinea l'importanza di una adeguata formazione e sensibilizzazione sulla sicurezza informatica, al fine di prevenire gli attacchi e minimizzare i danni in caso di incidenti. (Relazione Annuale DIS, 2022)

Le sfide future per la sicurezza informatica richiedono un costante adattamento e innovazione. Poiché gli attaccanti continuano a sviluppare nuove tattiche e tecniche, la comunità della sicurezza informatica deve lavorare incessantemente per sviluppare nuove strategie di difesa. Allo stesso tempo, è fondamentale che

l’industria, il governo e le organizzazioni in generale lavorino insieme per migliorare la sicurezza dei sistemi informatici.

Le organizzazioni devono sviluppare una comprensione profonda delle minacce emergenti, valutando costantemente le proprie difese e cercando di migliorare la loro resilienza. Le possibili evoluzioni degli attacchi informatici richiedono un approccio proattivo alla sicurezza informatica, che vada oltre la semplice reazione agli attacchi. Ciò include l’implementazione di pratiche di sicurezza solide, la formazione del personale su possibili minacce e l’uso di tecnologie avanzate per prevenire, rilevare e rispondere agli attacchi.

In conclusione, mentre le sfide future per la sicurezza informatica possono sembrare scoraggianti, offrono anche l’opportunità di innovare e migliorare. Con la giusta preparazione e strategia, è possibile difendersi dalle minacce emergenti e mantenere i sistemi informatici sicuri.

Le sfide future per la sicurezza informatica richiederanno nuovi approcci e strategie per proteggere le reti e le informazioni. Anticipare e prepararsi per queste minacce emergenti sarà cruciale al fine di mantenere la sicurezza nell’era digitale.

Tassonomia delle principali sfide future della *cybersecurity*

Intelligenza artificiale (AI) nelle minacce informatiche: L’uso dell’AI da parte degli attaccanti potrebbe rendere le minacce più sofisticate e difficili da rilevare, richiedendo l’implementazione di soluzioni di sicurezza basate sull’AI per contrastarle.

Cyber-attacchi su infrastrutture critiche: Le infrastrutture critiche come reti energetiche, sistemi di trasporto e servizi sanitari sono sempre più interconnesse e digitalizzate, rendendole potenziali bersagli per attacchi che potrebbero causare gravi conseguenze.

Internet delle Cose (IoT) non sicuro: L'espansione dell'IoT comporta una maggiore esposizione a rischi di sicurezza, poiché molti dispositivi IoT non vengono adeguatamente protetti, aprendo la porta a violazioni dei dati e a possibili attacchi alla privacy.

Minacce emergenti come l'intelligenza artificiale manipolata (*AI-based Manipulation*) e le minacce a Internet basate sul machine learning (*Machine Learning-based Threats*): Queste nuove minacce sfruttano l'AI, il *machine learning* (ML), gli algoritmi di riconoscimento facciale, la computer grafica e le reti neurali generative per manipolare informazioni, creare *deepfake* convincenti e sviluppare attacchi personalizzati.

Protezione dei dati nel cloud: Con l'aumento dell'adozione del cloud computing, la protezione dei dati e la gestione delle identità e degli accessi sono diventate priorità critiche, in quanto i dati possono essere esposti a rischi sia durante la trasmissione che durante l'archiviazione.

Domanda crescente di professionisti esperti in sicurezza informatica: questa supera l'offerta, creando una sfida nella formazione e nel reclutamento di personale qualificato per contrastare le minacce emergenti.

Leggi e normative in continua evoluzione: Le leggi sulla *privacy* e le normative sulla sicurezza informatica continuano a evolversi per affrontare le nuove minacce e proteggere i dati, creando sfide per le organizzazioni nell'adattamento e nella conformità alle nuove normative

Tassonomia delle principali prospettive future della cybersecurity

Integrazione della sicurezza nell'architettura delle applicazioni: Verso un approccio "*security by design*" delle organizzazioni, integrando la sicurezza fin

dalla fase di progettazione delle applicazioni e dei sistemi, per ridurre le vulnerabilità e migliorare la protezione.

Intelligenza artificiale per la difesa cibernetica: L'utilizzo dell'AI per rilevare, analizzare e rispondere alle minacce informatiche diventerà sempre più diffuso, consentendo una risposta più rapida ed efficace alle violazioni.

Blockchain per la sicurezza: La tecnologia *blockchain* potrebbe essere applicata per garantire la sicurezza e l'integrità dei dati, migliorando la protezione contro le frodi, le manipolazioni e gli accessi non autorizzati.

Sicurezza nel *cloud computing*: Le soluzioni di sicurezza per il cloud saranno sempre più avanzate, proteggendo i dati, le identità e gli ambienti di elaborazione cloud da attacchi e violazioni.

Sicurezza nell'era dell'Internet delle Cose (IoT): Le prospettive future includono soluzioni di sicurezza avanzate per l'IoT, come l'identificazione e l'eliminazione di dispositivi non sicuri, l'implementazione di protocolli crittografici robusti e l'adozione di *framework* di sicurezza specifici per l'IoT.

Sensibilizzazione e formazione continua: La sensibilizzazione alla sicurezza informatica e la formazione degli utenti saranno cruciali per creare una cultura della sicurezza e ridurre il rischio di attacchi basati su errori umani o ignoranza.

CAPITOLO 6 – CASI DI STUDIO

Nota Metodologica

Ai fini della nostra analisi di valutazione delle modalità di attacco sono stati esaminati 6 attacchi subiti da IC/OSE italiane ed estere che hanno avuto impatti in ambito cibernetico e, in alcuni casi, anche cinetico (sistemi OT).

Per analizzare gli attacchi cibernetici e cinetici è possibile utilizzare diversi *framework* e metodologie. La scelta del *framework* dipende dalle specifiche esigenze dell'analisi e dalla tipologia di attacco da analizzare. In questa tesi, verranno utilizzati uno o più *framework* specifici per l'analisi degli attacchi cibernetici e cinetici, che possano descrivere la catena dell'attacco dalle fasi di pianificazione, esecuzione e valutazione

Per dimostrare questa tesi il lavoro è stato organizzato mediante un'attività di analisi di *Intelligence* attraverso l'applicazione del ciclo informativo in 4 fasi: direzione, ricerca informativa, elaborazione e disseminazione (Conio, 2020) e l'utilizzo di fonti *Open Source Intelligence* (OSINT), ovvero attraverso l'analisi delle informazioni provenienti da fonti aperte da banche dati pubbliche e dal *deep web* (Lapi, 2021).

Inoltre, a seconda dei casi analizzati, saranno applicate ulteriori tecniche di analisi strutturata, tra le quali: un modello di classificazione generale degli attacchi *cyber* e un modello di analisi delle catene di attacco (Jusas, 2019). Quest'ultimo risulta utile per comprendere come gli attaccanti abbiano compromesso il sistema informatico e identificare le aree che richiedono maggiore attenzione nella sicurezza o per le quali poter sviluppare contromisure efficaci per mitigare gli effetti dell'attacco e prevenire attacchi futuri simili.

L'Analisi delle catene di attacco (in inglese *Attack Chain Analysis*) è una tecnica di analisi strutturata utilizzata in ambito informatico per comprendere il ciclo di

vita di un attacco, dalla fase di ricognizione alla fase di post-attacco. L'obiettivo dell'analisi delle catene di attacco è di identificare le singole fasi dell'attacco e le tecniche utilizzate dall'attaccante, al fine di sviluppare una comprensione completa della minaccia e delle contromisure necessarie per mitigarne gli effetti.

Il modello di *Attack Chain Analysis* (figura 13) solitamente prevede 7-9 fasi. Tuttavia, a seconda delle fonti, potrebbero esserci delle variazioni o delle sottocategorie all'interno di queste fasi. In generale, le fasi si dividono in 4 stadi: sociale, iniziale, di transizione e finale

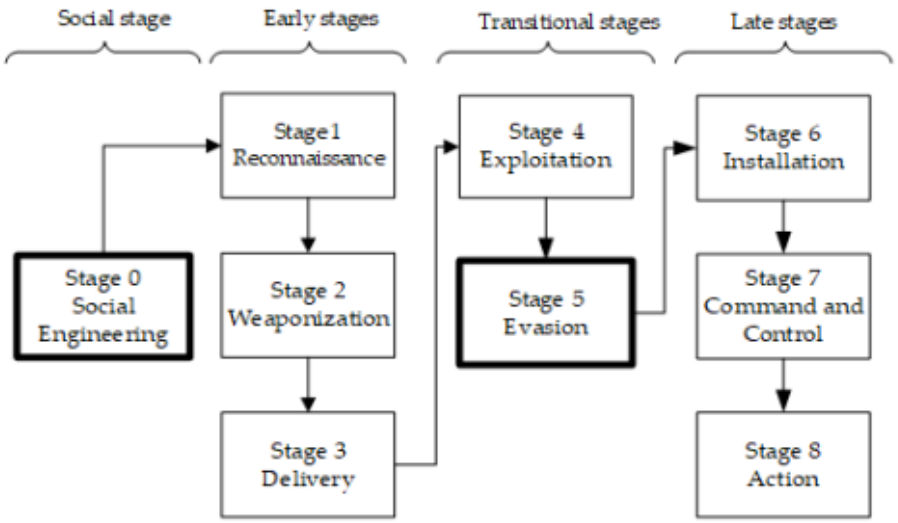


Figura 13 – Esempio di modello delle fasi della catena di attacco © 2019 Jusas

Secondo il modello generico, le fasi sono le seguenti:

1. ***Reconnaissance* (Ricognizione)**: Durante questa fase, gli attaccanti cercano di raccogliere informazioni sul sistema *target*, come indirizzi IP, porte aperte, configurazioni di rete e altre informazioni rilevanti per pianificare l'attacco.
2. ***Weaponization* (Armamento)**: In questa fase, gli attaccanti sviluppano o selezionano gli strumenti e i malware necessari per eseguire l'attacco, il cosiddetto "*payload*". Possono *includere exploit, backdoor, malware* personalizzati o strumenti per l'intrusione nel sistema *target*.

3. ***Delivery* (Consegna)**: Durante questa fase, gli attaccanti consegnano il *payload* malevolo al sistema target. Ciò può avvenire attraverso varie vie, come e-mail di *phishing*, *download* di file infetti o siti web compromessi.
4. ***Exploitation* (Sfruttamento)**: Una volta consegnato il *payload*, gli attaccanti sfruttano le vulnerabilità o le debolezze presenti nel sistema *target* per ottenere l'accesso non autorizzato o eseguire comandi malevoli.
5. ***Installation* (Installazione)**: Dopo aver ottenuto l'accesso al sistema, gli attaccanti installano e configurano il *malware* o gli strumenti necessari per perseguire i loro obiettivi. Questo potrebbe includere l'installazione di *backdoor*, *keylogger* o altre forme di *software* malevoli.
6. ***Command and Control* (Comando e controllo)**: Gli attaccanti stabiliscono una comunicazione tra il sistema compromesso e un *server* di comando e controllo (C&C) remoto. Questo permette loro di controllare e gestire il sistema compromesso, inviare istruzioni e ricevere dati o informazioni sensibili.
7. ***Actions on Objective* (Azioni sull'obiettivo)**: In questa fase finale, gli attaccanti compiono azioni volte a raggiungere i loro obiettivi. Queste azioni possono variare a seconda del tipo di attacco e degli obiettivi specifici degli attaccanti, come il furto di dati, la distribuzione di *malware*, il danneggiamento dei sistemi o il raggiungimento di altri scopi malevoli.

Queste fasi rappresentano un percorso comune seguito dagli attaccanti durante un attacco informatico, ma è importante notare che ogni attacco può avere caratteristiche uniche in base agli obiettivi, alle tecniche e alle motivazioni degli attaccanti coinvolti.

ATTACCO WANNACRY (RANSOMWARE)

L'attacco *ransomware* WannaCry del 2017 è stato uno degli attacchi più significativi nella storia della *cyberwarfare*. Questo worm ransomware si è diffuso rapidamente in tutto il mondo, colpendo numerose reti informatiche, tra cui ospedali, imprese e istituzioni governative.

Il *worm* sfruttava una vulnerabilità nel sistema operativo Windows chiamata *EternalBlue*, che era stata precedentemente scoperta e sviluppata dalla *National Security Agency* (NSA) degli Stati Uniti. WannaCry si è diffuso attraverso Internet, sfruttando la vulnerabilità per infettare i computer non aggiornati e criptare i dati presenti al loro interno. Successivamente, richiedeva un pagamento in *bitcoin* come riscatto per ripristinare l'accesso ai dati criptati.

L'attacco ha colpito oltre 200.000 computer in 150 paesi, causando danni stimati in milioni di dollari. Numerosi ospedali sono stati costretti a interrompere le loro attività, cancellare interventi chirurgici e ritardare le cure ai pazienti. Alcune aziende hanno subito interruzioni delle attività, mentre le istituzioni governative hanno visto compromessi i loro sistemi e i dati sensibili.

Tra le varie vittime, l'Università Bicocca di Milano e il Sistema Sanitario Nazionale (NHS) inglese sono state tra le organizzazioni colpite. L'attacco ha causato problemi significativi ai computer di un laboratorio di informatica dell'Università Bicocca e la rete del NHS ha subito interruzioni nelle operazioni ed è stato necessario adottare misure di emergenza per gestire la situazione. Inoltre, l'attacco ha colpito anche organizzazioni di assistenza primaria e medici di base, portando a disagi per i pazienti e la necessità di dirottare le risorse verso altre strutture.

WannaCry ha evidenziato la vulnerabilità delle organizzazioni a livello globale nei confronti dei *ransomware* e l'importanza di mantenere i sistemi operativi e le applicazioni aggiornate con le patch di sicurezza più recenti. Ha anche messo in luce la necessità di disporre di robuste soluzioni di sicurezza informatica, tra cui *backup* regolari dei dati, protezione antivirus e formazione degli utenti per riconoscere e prevenire gli attacchi di phishing e ransomware.

Infine, questo attacco, per via del suo impatto significativo sulla sicurezza informatica globale, ha spinto le organizzazioni a prendere sul serio le minacce dei *ransomware* e ad adottare misure più rigorose per proteggere i loro sistemi e dati sensibili.

Classificazione generale dell'attacco
Numero di fasi
Inizialmente, c'è la fase di consegna del *payload*, seguita dalla compromissione iniziale, l'espansione laterale nella rete, l'esecuzione del comando e controllo, la crittografia dei file e infine la richiesta di riscatto.
Velocità di attacco
Si è diffuso rapidamente, sfruttando la vulnerabilità EternalBlue SMBv1 per infettare un gran numero di sistemi in tutto il mondo in poche ore
Tipologia di attacco
È un attacco di tipo *ransomware*, che crittografa i file sul sistema bersaglio e richiede un riscatto per ripristinarli
Tipologia di attaccante
È stato attribuito a un gruppo di attaccanti noto come Lazarus Group, che è stato collegato a varie attività malevoli, tra cui attacchi informatici a scopo finanziario e di spionaggio.
Obiettivo
L'obiettivo di WannaCry era principalmente finanziario, poiché cercava di estorcere denaro alle vittime attraverso il pagamento del riscatto per ottenere la

chiave di decifrazione dei file crittografati. Tuttavia, l'attacco ha anche avuto un impatto significativo sulle operazioni delle organizzazioni colpite, causando interruzioni dei servizi e perdite finanziarie.
Risorse finanziarie
Richiedeva il pagamento del riscatto in Bitcoin, una criptovaluta, per garantirsi l'anonimato e la difficoltà di rintracciamento delle transazioni.
Conseguenze
Ha avuto conseguenze significative a livello globale. Ha infettato decine di migliaia di sistemi in oltre 150 paesi, compromettendo organizzazioni di vari settori, inclusi servizi sanitari, aziende di telecomunicazioni e infrastrutture critiche. Ha causato interruzioni dei servizi, perdite finanziarie, danni alla reputazione delle organizzazioni coinvolte e un maggiore interesse per la sicurezza informatica a livello internazionale.

Analisi della catena di attacco

Reconnaissance (Ricognizione):
Il *malware* WannaCry è stato creato incorporando un *exploit* noto come EternalBlue, che sfrutta una vulnerabilità (MS17-010) del protocollo Server Message Block (SMB), porte 445 e 139, di Windows. Seppur sia stata rilasciata una *patch* di aggiornamento per questa vulnerabilità, i sistemi afferenti al mondo della produzione, della sanità e delle telecomunicazioni hanno un ciclo di aggiornamento più lento, quindi sono risultati più vulnerabili.
Weaponization (Armamento):
WannaCry è composto da due componenti: un *worm* e un *ransomware*. Il Worm replica automaticamente sé stesso in tutti i sistemi informatici vulnerabili al protocollo SMB (*Server Message Block*) non aggiornati, trovati sulla medesima rete. Il *ransomware*, crittografa tutti i file che trova con 175 differenti tipologie di estensioni e richiedere l'equivalente di 300 $ in *Bitcoin* per ogni postazione

colpita. La richiesta di riscatto è contenuta nel file di testo *@Please_Read_Me@* ed è scritta in diverse lingue. Sul sistema infetto viene anche installato il *software* per poter decifrare i file (Wana Decryptor) ma lo si può utilizzare solo dopo aver pagato il riscatto. Se il riscatto non viene pagato entro 3 giorni, la cifra sale a 600 $. Se non viene pagato in 7 giorni allora tutti i file cifrati sono perduti.
Delivery (Consegna):
È stato diffuso attraverso internet, quindi inizia a cercare computer vulnerabili tentando di effettuare una connessione a un URL specifico, in particolare quelli che non hanno applicato una patch di sicurezza rilasciata da Microsoft per la vulnerabilità SMB (che è un protocollo di rete che permette la condivisione di file e stampanti tra nodi su una rete) e che quindi hanno la porta 445 aperta. Se la porta è aperta e il sistema non è stato aggiornato con la *patch*, WannaCry può sfruttare una nota vulnerabilità attraverso la creazione di un processo per ogni IP trovato nella sottorete LAN al fine di enumerare le interfacce di rete e tutte quelle raggiungibili nella rete. Se la connessione avviene, allora viene lanciato *l'exploit* e il sistema remoto viene infettato. Nelle prime varianti, il codice sorgente conteneva una richiesta Open_Internet (*non-proxy*[27]) verso un sito pubblico, noto come "*kill switch*", che era utilizzato per impedire la propagazione del malware. La richiesta di connessione a un dominio era "www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com". Se il dominio fosse stato raggiungibile, il malware avrebbe smesso di diffondersi. Questo meccanismo di "*kill switch*" è stato sfruttato in seguito per bloccare la diffusione del WannaCry.
Exploitation (Sfruttamento):
Il codice sfrutta la *backdoor DoublePulsar* e una vulnerabilità nota come *EternalBlue* nel protocollo *Server Message Block* (SMB) di Windows. Questa vulnerabilità permette al malware di diffondersi all'interno delle reti senza

[27] Raggiungere un sito web pubblico senza passare attraverso un proxy

interazione umana. Una volta che un sistema è infetto, WannaCry si auto-esegue. Inizia il processo di crittografia dei file dell'utente, rendendoli inaccessibili.
Installation (Installazione):
Il worm si auto-replica lateralmente nelle reti locali e remotamente attraverso *Internet*. Non è richiesta alcuna interazione umana per la diffusione del *malware*.
Command and Control (Comando e controllo):
Viene creato crea un nuovo servizio (chiamato mssecsvc2.0) che si copia in C:\Windows e si scrive nel registro di Windows per essere lanciato ad ogni avvio. Questo è un sistema utilizzato per mantenere la persistenza su di un sistema infetto attraverso la diffusione del *payload* WannaCry. Nasconde i propri file, attraverso l'assegnazione dell'attributo "*hidden*". Così ottiene tutti i privilegi per le sue sottodirectory. Un altro processo esegue la scansione ogni 3 secondi se carpire se sia stata collegata una nuova unità. In tal caso, tenta anche di infettarla. Inoltre, crea copie di *backup* dei file originali dell'utente generando una nuova chiave AES a 128 bit per ogni file, per far sì che ogni file sia crittografato con una chiave diversa. La crittografia utilizza la modalità CBC, con vettore di inizializzazione NULL. I file risultano quindi non leggibili e contengono un'estensione ".WCRY" dopo il nome file. Per poter decifrare i file, WannaCry invia la chiave privata crittografata del sistema infettato al server di Comando & Controllo dell'aggressore attraverso un canale segreto (TOR).
Actions on Objective (Azioni sull'obiettivo)
Utilizza una crittografia a chiave asimmetrica RSA a 2048 bit del sistema infettato. Quindi cifra tutte le chiavi AES con la chiave pubblica Crea una coppia di chiavi pubblica e privata, utilizza la chiave pubblica per crittografare i file del sistema infetto e poi cripta la chiave privata con un'altra chiave pubblica (dell'attaccante) incorporata nel codice del malware. Ogni file viene crittografato con una chiave unica, che viene poi crittografata con la chiave pubblica del malware. Dopo che tutti i file sono stati crittografati, WannaCry

mostra un messaggio di riscatto all'utente, richiedendo il pagamento in Bitcoin per la chiave di decifrazione.

L'utente che desidera recuperare i suoi file deve pagare un riscatto in *Bitcoin*. Quando effettua il pagamento, invia anche l'ID univoco del suo portafoglio Bitcoin agli aggressori. Questo permette agli aggressori di identificare il pagamento e di sapere a quale computer corrisponde.

Se gli aggressori confermano il pagamento, restituiscono la chiave privata del sistema infetto in chiaro. Questa chiave può essere utilizzata per decifrare i file sul computer infetto.

L'utente invia quindi l'ID univoco del suo portafoglio *Bitcoin*, in modo da consentire agli aggressori di identificare il suo pagamento. Se il pagamento viene confermato, l'aggressore restituisce la chiave privata del sistema che è stato infettato, in chiaro.

Conclusioni/Lezioni apprese
Questo attacco ha dimostrato la necessità di mantenere costantemente aggiornati i sistemi informatici per garantire la sicurezza dei propri dati e della propria attività. Cosa fare per proteggersi: - disabilitare il protocollo SMBv1. - Mantenere tutti i sistemi Windows aggiornati all'ultima versione delle patch di protezione relative al bollettino di sicurezza MS17-010 del 14 marzo 2017. - Se possibile, bloccare il traffico sulla porta 445. - Tenere aggiornato il *software antivirus.* - Eseguire aggiornamenti di sicurezza degli apparati di rete. - Predisporre procedure di *backup* sicure utilizzabili anche se la rete è disabilitata.

- educare gli utenti sui pericoli del *phishing*, degli attacchi *watering hole* e dell'uso di *software* non sicuri/non controllati.
- utilizzare programmi anti-malware con funzionalità anti-ransomware
- mantenere aggiornati i software *anti-malware* e *firewall.*

Fonti

- Akbanov, M., Vassilakis, V. G., & Logothetis, M. D. (2019). WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. Journal of Telecommunications and Information Technology, (1), 113-124.
- Brambilla (Assiteca Sicurezza Informatica), (2017), Vademecum WannaCry: cos'è e come proteggersi https://www.assiteca.it/wp-content/uploads/2017/05/WannaCry-VADEMECUM-15.05.17.pdf
- CCDCOE (NATO Cooperative Cyber Defence Centro of Excellence), (2017), WannaCry Campaign: Potential State Involve-ment Could Have Serious Consequences, https://ccdcoe.org/news/2017/wannacry-campaign-potential-state-involvement-could-have-serious-consequences/
- Deng, Y., Lambrecht, A., & Tucker, C. E. (2020). Asymmetric Consequences of Cyber-Vulnerability on Health Services. Available at SSRN 3642485.
- Di Giuseppe C. (2022) Il ransomware Wannacry https://www.analisidifesa.it/2022/05/il-ransomware-wannacry/
- Ferla D. (2020), WannaCry Dissected, an in-depth analysis of the malware outbreak, Università di Bologna, http://www.lia.deis.unibo.it/Courses/SicurezzaM1920/lab/lab00_wannacry.pdf
- Ferla D. (2020), WannaCry Dissected, an in-depth analysis of the malware outbreak, Università di Bologna, http://www.lia.deis.unibo.it/Courses/SicurezzaM1920/lab/lab00_wannacry.pdf
- Kao, D., Hsiao, S., & Tso, R. (2019). Analyzing WannaCry Ransomware Considering the Weapons and Exploits. 2019 21st International Conference on Advanced Communication Technology (ICACT), 1098-1107.

- Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2022). Ransomware detection, avoidance, and mitigation scheme: A review and future directions. Sustainability, 14(1), 8. doi:https://doi.org/10.3390/su14010008
- Malik, S., & Kumar Agrawal, A. Multi Pronged Approach for Ransomware Analysis. Available at SSRN 4017025.
- Mandrioli, D. (2018). Il caso WannaCry: il fenomeno dei cyber attacks nel contesto della responsabilità internazionale degli Stati. Il caso WannaCry: il fenomeno dei cyber attacks nel contesto della responsabilità internazionale degli Stati, 473-492.
- National Audit Office (NAO), (2018), Investigation: WannaCry cyber attack and the NHS, Department of Health, HC 414 SESSION 2017–2019 25 APRIL 2018
- Trautman, L. J., & Ormerod, P. C. (2018). Wannacry, ransomware, and the emerging threat to corporations. Tenn. L. Rev., 86, 503.

ATTACCO A SOLARWINDS (*SUPPLY CHAIN*)

L'attacco, rilevato alla fine del 2020, è stato uno dei più sofisticati e diffusi attacchi alla *supply chain*. Gli aggressori (definito col nome dell'APT Solorigate) hanno infettato il *software* di gestione della rete e risorse IT "Orion" di SolarWinds.
Questo *software* era ampiamente utilizzato da oltre 30.000 organizzazioni, tra cui enti pubblici, aziende private e agenzie governative. Il *malware* Sunburst è stato inserito all'interno degli aggiornamenti del *software* Orion, sfruttando una vulnerabilità *zero-day* della piattaforma. Di conseguenza, molte organizzazioni che hanno installato gli aggiornamenti infetti hanno subito l'infezione. Tuttavia, solo i server connessi a internet si sono infettati in quanto hanno stabilito un dialogo col sistema di comando & controllo dell'attaccante. Inoltre, vi è il sospetto che, già mesi prima dell'attacco, *hacker* cinesi (APT Nobelium) avrebbero avuto accesso si sistemi del Dipartimento dell'Agricoltura degli Stati Uniti, non tramite Sunburst bensì tramite altri malware, quindi sfruttando la medesima vulnerabilità *zero-day*.
Tornando all'evento di fine 2020, il *malware*, inizialmente dormiente, dopo un periodo di latenza, è stato successivamente attivato, permettendo agli aggressori di eseguire comandi, raccogliere dati sensibili e lanciare ulteriori attacchi. L'attacco ha colpito molte organizzazioni di primo piano, tra cui agenzie governative statunitensi, causando significative preoccupazioni sulla sicurezza dei dati e delle infrastrutture IT.
L'attacco SolarWinds ha evidenziato la vulnerabilità della catena di approvvigionamento del software, mettendo in discussione la sicurezza dei fornitori e la fiducia nelle loro soluzioni. Ha anche sollevato la necessità di migliorare le difese contro attacchi cibernetici avanzati, come l'utilizzo di vulnerabilità *zero-day* per infiltrarsi nei sistemi. Questo evento ha portato a un rinnovato focus sulla sicurezza della catena di approvvigionamento del *software* e

sull’importanza di implementare rigorose misure di protezione e di verifica dei fornitori.

Classificazione generale dell’attacco
Numero di fasi
Infiltrazione iniziale, *backdoor* nell’applicativo *software* Orion, aggiornamenti compromessi, diffusione ai clienti di SolarWinds, escalation dei privilegi, furto di dati e copertura delle tracce.
Velocità di attacco
È stato un attacco molto lento e metodico. I cybercriminali hanno avuto accesso ai sistemi SolarWinds per diversi mesi prima che l’attacco venisse scoperto. Questo ha permesso loro di coprire le proprie tracce e di approfondire l’accesso ai sistemi.
Tipologia di attacco
L’attacco è considerato un attacco di "*Supply Chain*" e un attacco di *Advanced Persistent Threat* (APT). Un attacco alla s*upply chain* avviene quando un aggressore si infiltra in un sistema compromettendo un componente della catena di fornitura del sistema (in questo caso, il software Orion).
Tipologia di attaccante
L’attacco pare sia stato attribuito a un gruppo di cyber-criminali (*State sponsored actor*), di matrice russa (APT29 “*Cozy Bear*”). Tuttavia, non vi sono ancora certezze sull’effettiva attribuzione dell’attacco.
Obiettivo
Gli obiettivi dell’attacco, per finalità di spionaggio, includevano agenzie governative, società di telecomunicazioni, società di consulenza, tecnologia e petrolio negli Stati Uniti e in altri paesi, Italia compresa.
Risorse finanziarie
Essendo un attacco sponsorizzato da un presunto Stato, è probabile che dietro ci fossero risorse finanziarie significative. Inoltre, la sofisticazione dell’attacco

suggerisce una notevole competenza tecnica e risorse per eseguire l'attacco su larga scala.
Conseguenze
L'attacco ha avuto gravi conseguenze sulla sicurezza nazionale degli Stati Uniti e di altri paesi. Ha esposto un gran numero di dati sensibili e potenzialmente ha compromesso l'integrità di molti sistemi informatici. Ha anche evidenziato la vulnerabilità delle catene di fornitura di *software* alle minacce di sicurezza.

Analisi della catena di attacco

Reconnaissance (Ricognizione):
Gli aggressori sono riusciti a infiltrarsi nel sistema di costruzione del *software* di gestione di rete "Orion", di fatto una vulnerabilità *zero-day*, che viene utilizzato per compilare e distribuire gli aggiornamenti dello stesso attraverso il furto di credenziali tramite un attacco di *phishing*. Tuttavia, l'autore della minaccia non ha modificato il *repository* di codice sorgente ma l'attività si è concentrata all'interno dell'ambiente di creazione automatizzata del software (SUNSPOT).
Weaponization (Armamento):
L'attacco è stato preparato creando un malware, noto come Sunburst, che è stato incorporato nel *software*. Una volta all'interno del sistema di costruzione del *software*, gli aggressori sono stati in grado di inserire il *malware* nel codice sorgente.
Delivery (Consegna):
Quando SolarWinds ha distribuito i suoi aggiornamenti software periodici della piattaforma Orion, il *malware* è stato distribuito (inconsapevolmente) a tutti i clienti che hanno installato l'aggiornamento, infettando così i loro sistemi.
Exploitation (Sfruttamento):
Il *malware* era configurato per rimanere dormiente per un periodo di tempo dopo l'installazione, per evitare di rilevare l'attacco. Dopo questo periodo, il *malware*

si attiva e inizia a comunicare con i server di comando e controllo (C&C) degli aggressori.
Installation (Installazione):
Una volta attivato, il *malware* può eseguire comandi da parte degli aggressori, permettendo loro di eseguire ulteriori attacchi, come l'escalation dei privilegi e il movimento laterale all'interno della rete per raccogliere informazioni sensibili, come credenziali di accesso e acquisire ampio accesso a dati sensibili e ai sistemi informatici infettati.
Command and Control (Comando e controllo):
Sunburst, una volta attivato, cominciava a comunicare coi server degli attaccanti. Questa connessione riusciva ad eludere la possibilità di essere rilevata attraverso il mascheramento, di conseguenza sembrava normale traffico di rete. I dati sensibili sono stati quindi esfiltrati e trasferiti sui server dei criminali. La connessione tra i *server* C&C e i sistemi infettati permetteva anche di scatenare ulteriori attacchi, scaricando altri strumenti di *hacking* o *malware*, eseguire comandi sulle macchine infette o muoversi lateralmente attraverso la rete locale (del server infetto) al fine di espandere i privilegi, sfruttare ulteriori vulnerabilità, utilizzare strumenti di amministrazione come *PowerShell*, eseguire altri attacchi di *phishing* o di ingegneria sociale, rubare altre credenziali.
Actions on Objective (Azioni sull'obiettivo)
Il malware viene utilizzato per raccogliere informazioni dai sistemi infetti, come informazioni sulla configurazione del sistema, informazioni sull'account e dati di rete. Una volta raccolti vengono inviati di nuovo ai server C&C degli aggressori attraverso una connessione di rete criptata. Infine, gli aggressori cercano di cancellare le tracce del loro attacco per evitare di essere scoperti. Ad esempio, potrebbero disattivare o rimuovere il *malware*, cancellare i log del sistema che mostrano la loro attività, o utilizzare altri metodi per mascherare la loro presenza.

Conclusioni/Lezioni apprese
Cosa fare per proteggersi: - Mantenere aggiornate le *patch* di sicurezza. Assicurarsi costantemente di installare gli aggiornamento software e le ultime patch dei fornitori. - Monitorare il codice attraverso l'implementazione di misure di sicurezza come il controllo del codice sorgente, l'analisi statica e dinamica dello stesso al fine di rilevare eventuali modifiche, variazioni o anomalie che potrebbero rappresentare delle compromissioni. - Applicare il principio del minimo privilegio, limitando gli accessi del personale alle risorse critiche e attivare la *multi-factor authentication* per gli utenti con particolari privilegi amministrativi. - Effettuare regolarmente il *backup* dei dati critici e testare i piani di sicurezza e di ripristino. - Condividere coi partner le best practice di gestione della sicurezza per aumentare la sicurezza della *supply chain*. - Utilizzare strumenti di monitoraggio quali EDR e SIEM. - Controlli di accesso e autenticazione: Implementare misure di autenticazione forte, come l'uso di fattori multipli o l'autenticazione a due fattori (2FA), per proteggere l'accesso ai sistemi e alle risorse sensibili. - Isolare dalla rete i sistemi compromessi dal *malware*. La lezione appresa da questo attacco consiste nell'l'importanza di adottare una mentalità di difesa in profondità, che include una valutazione rigorosa della sicurezza dei fornitori, la scansione continua dei sistemi per rilevare minacce avanzate e una risposta rapida e coordinata in caso di violazioni. La *cybersecurity* deve essere considerata come una priorità strategica in ogni organizzazione per affrontare le sfide sempre crescenti dei moderni attacchi informatici.
Fonti
- Centre for Cybersecurity (CFCS) of Denmark, (2021), SolarWinds: State-sponsored global software supply chain attack

- Clusit Community for Security, (2022), SUPPLY CHAIN SECURITY L'importanza di conoscere e gestire i rischi della catena di fornitura, Supply Chain Security
- CSIRT, (2020), SUNBURST Threat Report, ACN – Agenzia per la Cybersicurezza Nazionale
- Devanny, J., Martin, C., & Stevens, T. (2021). On the strategic consequences of digital espionage. Journal of Cyber Policy, 6(3), 429-450.
- ENISA (European Union Agency for Cybersecurity), (2021), ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS
- Huddleston, J., Ji, P., Bhunia, S., & Cogan, J. (2021, December). How VMware Exploits Contributed to SolarWinds Supply-chain Attack. In 2021 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 760-765). IEEE.
- Marcus Willett (2021) Lessons of the SolarWinds Hack, Survival, 63:2, 7-26, DOI: 10.1080/00396338.2021.190600
- Marelli, M. (2022). The SolarWinds hack: Lessons for international humanitarian organizations. International Review of the Red Cross, 104(919), 1267-1284.
- Mendola C., (2021), Lessons Learned from the SolarWinds Hack: What Went Wrong & How Can Lawyers Help Mitigate the Risk of Cyberattacks
- Miller, J. F. (2013). Supply chain attack framework and attack patterns. MITRE CORP MCLEAN VA.
- NIST (National Institute of Standards and Technology), (2021), Defending Against Software Supply Chain Attacks, Cybersecurity and Infrastructure Security Agency
- Raponi, S., Caprolu, M., & Di Pietro, R. (2021). Beyond SolarWinds: The Systemic Risks of Critical Infrastructures, State of Play, Future Directions. ITASEC, 21, 07-09.
- Sterle, L., & Bhunia, S. (2021, October). On solarwinds orion platform security breach. In 2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI) (pp. 636-641). IEEE.

ATTACCO ALLA RETE ELETTRICA UCRAINA (OT)

L'attacco da parte del *malware BlackEnergy* (versione 3) del 24 dicembre 2015 è stato un evento significativo che ha segnato un punto di svolta nella *cybersecurity*. Gli attaccanti hanno sfruttato il malware *BlackEnergy*, inizialmente progettato come strumento di attacco DDoS, ma successivamente modificato in uno strumento APT (*Advanced Persistent Threat*), per lanciare un attacco a *spear-phishing* contro tre fornitori di energia in Ucraina, tre infrastrutture critiche.

Attraverso un attacco *spear-phishing*, gli aggressori sono riusciti ad ottenere l'accesso ai sistemi informatici e di controllo industriale (SCADA) delle aziende, mappare la rete e raccogliere credenziali sensibili. Successivamente, hanno interrotto l'erogazione dell'energia elettrica spegnendo sottostazioni remote e causando un *blackout* che ha colpito circa 230.000 persone per diverse ore. In particolare, sette sottostazioni da 110 kV e ventitré da 35 kV sono state disconnesse per tre ore. Successivamente è emerso che l'attacco informatico ha colpito anche altre parti della rete di distribuzione e ha costretto gli operatori a passare alla modalità manuale. Poco dopo l'attacco, i funzionari governativi ucraini hanno dichiarato che le interruzioni erano state causate da un attacco informatico e che i servizi di sicurezza russi erano responsabili degli incidenti.
Questo attacco ha dimostrato che gli attacchi informatici possono avere conseguenze dirette sulla vita delle persone e sull'economia di un intero paese.

Infatti, l'attacco *BlackEnergy* è stato uno dei primi ad avere un impatto fisico diretto su un'infrastruttura critica su larga scala, evidenziando seriamente le vulnerabilità dei sistemi di controllo industriale alle minacce cibernetiche. Questo evento ha attirato l'attenzione sulle vulnerabilità dei sistemi di controllo industriale e ha evidenziato la necessità di una maggiore sicurezza e protezione per le infrastrutture critiche.

Da allora, gli attacchi contro le infrastrutture critiche sono diventati una preoccupazione sempre più grande per i governi e le organizzazioni di tutto il mondo. La protezione delle infrastrutture critiche è diventata una priorità strategica, con molti paesi che cercano di rafforzare le difese e sviluppare politiche e normative specifiche per mitigare queste minacce.

BlackEnergy ha anche messo in luce la necessità di proteggere non solo i sistemi informatici, ma anche i sistemi di controllo industriale e le reti di infrastrutture critiche. Spesso, queste infrastrutture utilizzano tecnologie *legacy* e presentano vulnerabilità significative. Pertanto, la sicurezza degli ambienti OT (Operational Technology) è diventata un aspetto cruciale della difesa cibernetica, richiedendo approcci specifici e soluzioni avanzate per mitigare le minacce.

Classificazione generale dell'attacco
Numero di fasi
L'attacco è stato un'operazione a più fasi. Ha iniziato con una campagna di *spear-phishing*, seguita dall'installazione del malware *BlackEnergy* 3 nei sistemi delle aziende energetiche e la manipolazione di documenti di Microsoft Office contenenti il *malware* per ottenere un punto di appoggio nelle reti IT. Successivamente, gli attaccanti hanno eseguito una fase di riconoscimento e mappatura della rete, acquisito le credenziali e infine lanciato l'attacco che ha portato all'interruzione dell'energia operando, non solo nelle infrastrutture collegate alla rete, come gli UPS (sistemi di autoalimentazione) ma anche nel saper operare i sistemi di controllo ICS attraverso un ulteriore sistema di controllo di supervisione. Inoltre, gli attaccanti hanno dimostrato la capacità e la volontà di prendere di mira i dispositivi di campo presso le sottostazioni, scrivere firmware malevoli personalizzati e rendere i dispositivi, come i convertitori *serial-ethernet*, inoperabili e irrecuperabili. In parallelo, si sono serviti anche dei sistemi telefonici per generare migliaia di chiamate al centro di assistenza

dell’azienda energetica per non permettere ai clienti di segnalare interruzioni del servizio.
Velocità di attacco
La velocità dell’attacco è stata relativamente lenta e metodica. Gli attaccanti hanno dedicato settimane o forse mesi alla preparazione dell’attacco, compreso il tempo per l’invio degli email di *spear-phishing*, l’installazione del *malware*, la mappatura della rete e l’acquisizione delle credenziali. La capacità più forte degli aggressori non consisteva nella scelta degli strumenti o nella loro competenza, ma nella capacità di saper condurre operazioni di ricognizione a lungo termine necessarie per conoscere l’ambiente ed eseguire un attacco altamente sincronizzato, a più fasi e multi-sito.
Tipologia di attacco
Questo è un esempio di attacco APT (Advanced Persistent Threat), in cui gli aggressori hanno penetrato e monitorato i sistemi nel tempo per portare a termine un attacco mirato e sofisticato. L’attacco finale alla rete elettrica è stato eseguito tramite accesso remoto ai sistemi di controllo industriale (ICS). Tra le varie componenti sfruttate dagli attaccanti si possono riscontrare: • *Spear-phishing* per ottenere l’accesso alle reti aziendali delle centrali elettriche • Identificazione di *BlackEnergy* 3 presso ciascuno sito colpito • Furto di credenziali dalle reti aziendali • Utilizzo di VPN per accedere alla rete ICS • Utilizzo di strumenti di accesso remoto esistenti nell’ambiente o invio di comandi direttamente da una stazione remota simile a un HMI operatore • Dispositivi di comunicazione *serial-ethernet* colpiti a livello *firmware* • Utilizzo di un *KillDisk* modificato per cancellare il master boot record dei sistemi dell’organizzazione colpita e la cancellazione mirata di alcuni log • Utilizzo dei sistemi UPS per influire sul carico con un’interruzione del servizio

• Attacco al centro di assistenza telefonico
Tipologia di attaccante
L’attacco è stato attribuito a un gruppo di attaccanti noto come *SandWorm*, che si ritiene abbia legami con la Russia.
Obiettivo
L’obiettivo era causare interruzioni nell’erogazione dell’energia in Ucraina, cosa che è stata realizzata spegnendo sottostazioni elettriche in varie regioni.
Risorse finanziarie
Mentre le cifre esatte non sono note, è chiaro che l’attacco richiedeva un livello di competenza e risorse significativo. Non solo per sviluppare o acquisire il malware *BlackEnergy* 3, ma anche per condurre la campagna di *spear-phishing*, mappare la rete, acquisire le credenziali e pianificare e eseguire l’attacco finale.
Conseguenze
L’attacco ha avuto conseguenze gravi. Circa 230.000 persone sono rimaste senza energia per diverse ore. Inoltre, l’attacco ha evidenziato le vulnerabilità delle infrastrutture critiche agli attacchi cibernetici e ha rafforzato l’importanza della sicurezza cibernetica nei sistemi di controllo industriale.

Analisi della catena di attacco

Reconnaissance (Ricognizione):
Gli attaccanti hanno eseguito una ricognizione per identificare i fornitori di energia in Ucraina come obiettivi e comprendere meglio le loro reti. Non sono stati segnalati avvistamenti di attività di ricognizione prima del targeting delle aziende energetiche. Tuttavia, un’analisi delle tre organizzazioni colpite mostra che erano obiettivi particolarmente interessanti a causa dei livelli di automazione nel loro sistema di distribuzione, che consentiva l’apertura remota degli interruttori in diverse sottostazioni.
Weaponization (Armamento):

Gli attaccanti hanno creato email di *spear-phishing* con allegati malevoli che, una volta aperti, avrebbero installato il malware *BlackEnergy* nei sistemi degli obiettivi. Armando documenti di *Microsoft Office* (*Excel* e *Word*) con *BlackEnergy* 3 all'interno dei documenti ne è stato possibile l'invio via mail al personale interno alla rete amministrativa e IT.
Delivery (Consegna):
Le email di *spear-phishing* sono state inviate agli operatori di sistema delle aziende energetiche.
Exploitation (Sfruttamento):
Quando gli operatori hanno aperto gli allegati infetti, il *malware BlackEnergy* è stato installato nei loro sistemi. All'apertura di un documento compromesso, veniva visualizzato un popup che incoraggiava gli utilizzatori ad abilitare le macro nel documento. Questa caratteristica consentiva al malware di essere installato sul sistema della vittima.
Installation (Installazione):
Una volta installato, *BlackEnergy* ha iniziato a lavorare per gli attaccanti, consentendo loro di mantenere la persistenza sulla rete e preparandosi per la fase successiva. Nella fase di Installazione, il malware *BlackEnergy* 3 si collegava agli indirizzi IP di comando e controllo (C2) per consentire la comunicazione tra l'avversario e il *malware* e i sistemi infetti. Queste vie consentivano all'avversario di raccogliere informazioni dall'ambiente e di abilitare l'accesso. Gli attaccanti sembrano aver ottenuto l'accesso più di sei mesi prima del 23 dicembre 2015, quando si è verificato il *black-out*. Una delle loro prime azioni è stata la raccolta di credenziali, l'escalation dei privilegi e il movimento laterale all'interno dell'ambiente.
Command and Control (Comando e controllo):
Gli attaccanti hanno acquisito il controllo dei sistemi infetti e hanno iniziato a comunicare con loro per eseguire ulteriori operazioni. Grazie alle informazioni raccolte, gli aggressori potrebbero aver individuato le connessioni VPN ed aver

eseguito una mappatura della rete dei sistemi di controllo (ICS). Quindi, utilizzando connessioni e comandi nativi, potrebbero aver scoperto ed estratto i dati necessari per pianificare l'operazione distribuita su più siti e stazioni di produzione dell'energia arrivando fino a compromettere le regole di continuità di un UPS individuato nella stessa (disconnessione programmata degli UPS).
Actions on Objective (Azioni sull'obiettivo)
Gli attaccanti hanno mappato le reti delle aziende energetiche, raccolto le credenziali necessarie ed eseguito il loro obiettivo principale. Con le credenziali raccolte, gli attaccanti sono stati in grado di spostarsi lateralmente attraverso la rete, acquisendo l'accesso ai sistemi di controllo industriale (ICS) che governano la distribuzione dell'energia quindi hanno interrotto l'erogazione dell'energia spegnendo a distanza le sottostazioni elettriche e causando un blackout che ha interessato circa 230.000 persone per diverse ore. Questo ha comportato l'attuazione di differenti modalità di "attacco" da sito a sito e la compromissione di dispositivi (*serial-ethernet*) di controllo detta rete SCADA relativa alle sottostazioni (dirottamento delle funzionalità). Infine, è stato installato un *software* malevolo identificato come un *KillDisk* modificato o personalizzato in tutto l'ambiente per negare l'esecuzione di comandi di ripristino. In aggiunta, un attacco di *flooding* al centralino di assistenza telefonica non ha permesso di gestire le chiamate provenienti dagli utenti impattati dal problema.

Conclusioni/Lezioni apprese
L'attacco alla rete elettrica ucraina del 2015 ha rappresentato un punto di svolta nella comprensione del potenziale impatto dei cyber attacchi sulle infrastrutture critiche. Questo attacco ha dimostrato che le minacce cibernetiche non sono solo digitali, ma possono avere conseguenze fisiche gravi. Un attacco ben eseguito può causare *blackout*, interruzioni del servizio e altri danni fisici.

Un aspetto cruciale emerso è l'importanza della formazione del personale. L'attacco è infatti iniziato con una campagna di spear-phishing, sottolineando l'importanza di educare il personale a riconoscere e gestire in modo sicuro le email sospette.

L'incidente ha anche evidenziato la necessità di avere piani di risposta agli incidenti ben definiti e testati. Grazie alla loro preparazione, i fornitori di energia ucraini sono riusciti a ripristinare manualmente il servizio in poche ore.

Un'altra lezione appresa riguarda l'importanza della segmentazione della rete. Gli attaccanti sono stati in grado di spostarsi lateralmente attraverso la rete una volta penetrati nel sistema. La segmentazione della rete può limitare la capacità di un attaccante di accedere a parti critiche del sistema.

L'attacco ha inoltre evidenziato la necessità di proteggere i sistemi di controllo industriale (ICS) e SCADA. Questi sistemi spesso non sono progettati con la sicurezza in mente, il che li rende vulnerabili. Pertanto, questi sistemi richiedono protezioni specifiche e procedure di sicurezza.

È fondamentale mantenere tutti i sistemi e le applicazioni aggiornati con le ultime patch di sicurezza, come è stato dimostrato dallo sfruttamento di vulnerabilità note durante l'attacco.

Infine, l'attacco ha sottolineato l'importanza della cooperazione internazionale. Gli attacchi cibernetici possono attraversare i confini nazionali e, pertanto, la cooperazione internazionale è fondamentale per prevenire, rilevare e rispondere agli attacchi cibernetici.

Fonti

- Assante, M. J. (2016). Confirmation of a coordinated attack on the Ukrainian power grid. SANS Industrial Control Systems Security Blog, 207.
- Case, D. U. (2016). Analysis of the cyber attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC), 388, 1-29.
- Cherepanov, A., & Lipovsky, R. (2016). Blackenergy–what we really know about the notorious cyber attacks. Virus Bulletin October.

- Lehman, G., (2016), CYBER ATTACK AGAINST UKRAINIAN POWER PLANTS.
- Liang, G., Weller, S. R., Zhao, J., Luo, F., & Dong, Z. Y. (2016). The 2015 ukraine blackout: Implications for false data injection attacks. IEEE transactions on power systems, 32(4), 3317-3318.
- N. Kshetri and J. Voas, (2017), Hacking Power Grids: A Current Problem, in Computer, vol. 50, no. 12, pp. 91-95, December, doi: 10.1109/MC.2017.4451203.
- Petropulu, Athina and Diamantaras, Konstantinos I. and Han, Zhu and Niyato, Dusit and Zonouz, Saman, (2019), Contactless Monitoring of Critical Infrastructure [From the Guest Editors]" in IEEE Signal Processing Magazine, vol. 36, no. 2, pp. 19-21, March 2019, doi: 10.1109/MSP.2018.2890357.
- Rafiullah Khan, Peter Maynard and Kieran McLaughlin et al., (2016), Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid. DOI: 10.14236/ewic/ICS2016.7
- Shehod, A. (2016). Ukraine power grid cyberattack and US susceptibility: Cybersecurity implications of smart grid advancements in the US. Cybersecurity Interdisciplinary Systems Laboratory, MIT, 22, 2016-22.
- Sullivan, J. E., & Kamensky, D. (2017). How cyber-attacks in Ukraine show the vulnerability of the US power grid. The Electricity Journal, 30(3), 30-35.
- Tang, Yi and Qian Chen and Mengya Li and Wang, Qi and Ni, Ming and XiangYun Fu, (2016). Challenge and evolution of cyber-attacks in Cyber Physical Power System, IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), Xi'an, China, 2016, pp. 857-862, doi: 10.1109/APPEEC.2016.7779616.
- Yurtayeva, k, (2022), Cyberaggression as a part of hybrid war against ukraine. In кібербезпека в україні: правові та організаційні питання international scientific-practical conference" Cybersecurity in Ukraine: Legal and (p. 8).

ATTACCO (STUXNET) ALLE CENTRALI NUCLEARI IRANIANE

Stuxnet è un caso significativo nella storia della *cyber warfare*. W32.Stuxnet è un *worm* informatico altamente sofisticato scoperto nel 2010, noto per aver preso di mira i sistemi di controllo industriale (ICS) utilizzati nel programma nucleare iraniano. È stato progettato per riprogrammare i sistemi di controllo industriale al fine di sabotare le centrifughe impiegate nell'arricchimento dell'uranio, rappresentando così un attacco diretto a un'infrastruttura critica. In particolare, modificando il codice sui *programmable logic controller* (PLC), è stato possibile modificare le modalità di funzionamento delle centrifughe e nascondere tali modifiche all'operatore stesso.

Ciò che ha reso Stuxnet un'arma cibernetica senza precedenti è stata la sua complessità e la sua abilità nel penetrare e compromettere sistemi altamente protetti. Utilizzando quattro vulnerabilità *zero-day*, il *worm* è stato in grado di infettare i computer di controllo industriali e manipolare il funzionamento delle centrifughe, causando danni fisici alle apparecchiature. Questo ha rappresentato un punto di svolta nell'era della *Cyber Warfare*, dimostrando che gli attacchi informatici possono influenzare direttamente il mondo fisico e le infrastrutture critiche.

Stuxnet è stato sviluppato con una conoscenza approfondita dei sistemi di controllo industriale utilizzati nell'arricchimento dell'uranio, il che suggerisce l'implicazione di un attore con risorse e competenze significative. È stato ampiamente ipotizzato che Stuxnet fosse stato sviluppato da agenzie di intelligence statali, come gli Stati Uniti e Israele, anche se non ci sono state conferme ufficiali in merito.
La maggior parte delle infezioni è stata riscontrata in Iran.

Questo attacco ha sollevato gravi preoccupazioni sulla sicurezza delle infrastrutture critiche e ha evidenziato la necessità di protezione avanzata per i sistemi di controllo industriale. Ha mostrato che gli attacchi informatici possono essere utilizzati come strumento di guerra e hanno portato ad un aumento degli sforzi per rafforzare le difese cibernetiche e sviluppare politiche e normative specifiche per proteggere le infrastrutture critiche da futuri attacchi simili.

Inoltre, Stuxnet ha sollevato interrogativi sulla sicurezza informatica globale e ha spinto molti paesi a rivedere le proprie strategie di difesa cibernetica e ad investire in ricerca e sviluppo per mitigare le minacce provenienti dalla *cyber warfare*.

Classificazione generale dell'attacco
Numero di fasi
L'attacco Stuxnet è stato estremamente complesso e ha attraversato numerose fasi, compresa la creazione di un *malware* altamente sofisticato, l'infiltrazione nei sistemi di controllo industriale (ICS), la manipolazione dei processi industriali e infine l'autoeliminazione per evitare la rilevazione.
Velocità di attacco
Stuxnet è stato progettato per essere un attacco lento e persistente. Il *malware* era programmato per diffondersi lentamente e agire solo quando erano soddisfatte determinate condizioni, al fine di evitare la rilevazione.
Tipologia di attacco
Stuxnet è un esempio di un attacco APT (*Advanced Persistent Threat*). Sfruttava quattro vulnerabilità *zero-day* e usava tecniche di rootkit per rimanere nascosto. Il suo obiettivo era sabotare specifiche attività industriali piuttosto che rubare dati. A livello architetturale presenta molte caratteristiche, tra cui la capacità di auto-replicazione tramite dispositivi rimovibili sfruttando una vulnerabilità che permette l'esecuzione automatica dei file, la diffusione in una rete LAN

sfruttando una vulnerabilità nel servizio di stampa di Windows, l'esecuzione in computer remoti tramite condivisioni di rete, l'inserimento in progetti Step 7 per l'esecuzione automatica e l'aggiornamento tramite meccanismi *peer-to-peer* all'interno di una rete locale. Inoltre, Stuxnet sfrutta quattro vulnerabilità di Microsoft non ancora corrette, tra cui due per l'auto-replicazione e due per l'elevazione dei privilegi, contatta un server di controllo e comando per scaricare ed eseguire codice, contiene un *rootkit* per Windows per nascondere i suoi file binari, tenta di eludere i prodotti di sicurezza, riconosce un sistema di controllo industriale specifico e modifica il codice dei PLC Siemens per sabotare potenzialmente il sistema. Inoltre, nasconde il codice modificato sui PLC, essendo essenzialmente un *rootkit* per i PLC stessi.
Tipologia di attaccante
Stuxnet è generalmente attribuito a un'operazione congiunta tra gli Stati Uniti e Israele, sebbene ciò non sia mai stato ufficialmente confermato. Questo suggerisce un attacco stato-sponsorizzato con risorse significative a disposizione.
Obiettivo
L'obiettivo principale dell'attacco Stuxnet era interrompere il programma nucleare iraniano. Ha specificamente mirato alle centrifughe usate per l'arricchimento dell'uranio nelle strutture nucleari iraniane.
Risorse finanziarie
Stuxnet è uno degli attacchi cibernetici più sofisticati mai sviluppati, suggerendo che fosse finanziato a livello statale. La creazione del *malware*, l'identificazione delle vulnerabilità *zero-day* e il mantenimento dell'attacco avrebbero richiesto risorse finanziarie significative.
Conseguenze
L'attacco ha avuto successo nel causare danni fisici alle centrifughe iraniane, ritardando il loro programma nucleare. Tuttavia, ha anche portato a una maggiore consapevolezza della potenziale minaccia delle *Cyber Warfare* contro

le infrastrutture critiche e potrebbe aver contribuito a una corsa agli armamenti cibernetici.

Analisi della catena di attacco

Reconnaissance (Ricognizione):
Gli attaccanti hanno identificato gli obiettivi specifici e studiato i sistemi di controllo industriale (ICS) utilizzati nelle strutture nucleari iraniane. In particolare, hanno raccolto informazioni su WinCC e sul *software* Siemens Step7 utilizzato per controllare le centrifughe attraverso i controllori logici programmabili (PCL). I PLC sono dispositivi che controllano *l'hardware* meccanico e di processo in un impianto industriale.
Weaponization (Armamento):
Hanno sviluppato un malware estremamente sofisticato (W32.Stuxnet) che sfruttava quattro vulnerabilità *zero-day* non precedentemente note. Il *worm* era in grado di autoreplicarsi e di nascondersi nei sistemi infetti. Stuxnet ha infatti sfruttato le vulnerabilità per alterare il codice di programmazione dei PLC, causando danni fisici alle centrifughe iraniane usate nell'arricchimento dell'uranio. Inoltre, Stuxnet ha sfruttato altre vulnerabilità per diffondersi e mantenere la sua presenza nei sistemi infetti. Ad esempio, ha sfruttato una vulnerabilità *zero-day* nel sistema operativo Microsoft Windows per ottenere l'accesso iniziale ai computer bersaglio, tecniche di elusione degli antivirus, l'esecuzione di codice di iniezione e di "aggancio" dei processi, procedure di infezione di rete, aggiornamenti *peer-to-peer* e un'interfaccia di comando e controllo. Inoltre, Stuxnet è stato progettato per utilizzare più vettori di infezione, compresi dispositivi USB infetti e la propagazione attraverso le reti locali. Una volta infettato un sistema, il *worm* cercava di diffondersi nelle reti interne, sfruttando le *password* deboli o utilizzando le connessioni remote per infettare altri computer con il *malware*.

Stuxnet è un esempio notevole di un *malware* complesso che ha sfruttato una combinazione di vulnerabilità *zero-day*, tecniche di propagazione sofisticate e un obiettivo specifico per causare danni fisici alle infrastrutture critiche.
Delivery (Consegna):
Stuxnet è stato inizialmente diffuso tramite USB. La scelta di usare USB suggerisce che l'accesso fisico alle strutture nucleari iraniane era un elemento chiave dell'attacco. A questo proposito, è stata utilizzata una tecnica nota come "*autorun*". Il *worm* era progettato per copiarsi su una chiavetta USB quando veniva inserito in un computer infetto. Successivamente, quando la chiavetta USB veniva collegata a un altro computer, Stuxnet veniva automaticamente eseguito tramite la funzione di *autorun* di Windows, che avviava il worm senza richiedere l'interazione dell'utente. L'uso della diffusione tramite USB è stato un elemento chiave nella strategia di propagazione di Stuxnet, in quanto ha consentito al *worm* di diffondersi tra i sistemi non connessi a Internet e di raggiungere le reti interne delle infrastrutture critiche.
Exploitation (Sfruttamento):
Una volta nel sistema, Stuxnet ha sfruttato le vulnerabilità *zero-day* per ottenere il controllo dei sistemi. È stato in grado di farlo senza essere rilevato grazie all'uso di tecniche di rootkit.
Installation (Installazione):
Stuxnet si è installato autonomamente sui sistemi infetti attraverso un dispositivo removibile (USB) e per mezzo di un terzo soggetto consapevole o inconsapevole, e ha poi cercato di diffondersi attraverso la rete locale alla ricerca di computer utilizzati per programmare le PCL.
Command and Control (Comando e controllo):
Stuxnet non necessitava di un server di comando e controllo per agire. Il *worm* era programmato per agire autonomamente una volta che determinate condizioni erano soddisfatte. Stuxnet era in grado di muoversi lateralmente all'interno della rete per infettare altri sistemi e aumentare il suo impatto attraverso un metodo di

connettività *peer-to-peer*. Dopo aver completato il suo compito, Stuxnet si è auto-eliminato per evitare la rilevazione. Il *worm* ha anche usato tecniche di *rootkit* per nascondersi e rimanere nel sistema per il più tempo possibile.
Actions on Objective (Azioni sull'obiettivo)
Una volta in controllo dei sistemi di controllo industriale (ICS), Stuxnet ha iniziato a manipolare il funzionamento delle centrifughe, causandone il malfunzionamento e la distruzione.

Conclusioni/Lezioni apprese
L'attacco di Stuxnet ha rappresentato un momento cruciale nel panorama delle minacce alla sicurezza cibernetica, dimostrando che gli attacchi cibernetici possono avere impatti fisici significativi e duraturi. Ha rivelato l'importanza della sicurezza nei sistemi di controllo industriale (ICS), dato che prima di Stuxnet, la sicurezza ICS non era sempre una priorità. L'attacco ha messo in luce il fatto che i sistemi ICS sono obiettivi desiderabili e vulnerabili. Stuxnet ha sfruttato quattro vulnerabilità *zero-day*, cioè vulnerabilità non note al pubblico né al produttore del *software*. Questo ha evidenziato l'importanza delle attività di ricerca di vulnerabilità e del processo di divulgazione delle vulnerabilità. L'attacco è ampiamente considerato un *cyber-weapon*, probabilmente sviluppato da una nazione-stato. Questo solleva preoccupazioni sui potenziali impatti degli attacchi cibernetici quando sono utilizzati come parte di conflitti internazionali. Stuxnet è stato inizialmente diffuso tramite chiavette USB, evidenziando il ruolo che la sicurezza fisica gioca nella sicurezza cibernetica. Inoltre, ha dimostrato quanto sia importante avere piani di risposta alle emergenze in caso di attacchi cibernetici, specialmente per infrastrutture critiche.

Infine, Stuxnet è stato un attacco incredibilmente sofisticato, dimostrando che gli attaccanti sono sempre più capaci e disposti a investire risorse significative per raggiungere i loro obiettivi. In definitiva, Stuxnet ha segnato una nuova era nella cyber guerra, sottolineando la necessità di affrontare con serietà la sicurezza cibernetica, soprattutto per infrastrutture critiche e ICS.

Fonti

- Chen, T. M., & Abu-Nimeh, S. (2011). Lessons from stuxnet. Computer, 44(4), 91-93.
- Baezner, M., & Robin, P. (2017). Stuxnet (No. 4). ETH Zurich.
- Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. White paper, symantec corp., security response, 5(6), 29.
- Kushner, D. (2013). The real story of stuxnet. ieee Spectrum, 50(3), 48-53.
- Matrosov, A., Rodionov, E., Harley, D., & Malcho, J. (2010). Stuxnet under the microscope. ESET LLC (September 2010), 6.
- Perez, L. 8 Is Stuxnet the next Skynet? Autonomous cyber capabilities as lethal autonomous weapons systems. Artificial Intelligence and International Conflict in Cyberspace, 186.
- Jadhav, H., & Madoo, S. THE ETHICS OF CYBER WARFARE: EXPLORING THE USE OF CYBER ATTACK IN MILITARY OPERATIONS.
- Litvinov, E. A Undocumented feature or potential vulnerability?

ATTACCO (NETWALKER) A ENEL GROUP

L'attacco a ENEL Group mediante il *malware* Netwalker è stato un grave incidente di *cyber security* che ha coinvolto l'azienda energetica italiana nell'ottobre del 2020.
Nel corso dello stesso anno aveva già subito un altro attacco ma, in quel caso, le difese avevano funzionato.
In quello successivo, invece, i cybercriminali sono riusciti a infiltrarsi nei sistemi di ENEL e a criptare una vasta quantità di dati sensibili su progetti internazionali e architettura di centrali elettriche (4,54 TB poi finiti in parte sul *Dark web*), richiedendo un riscatto di circa 14 Milioni di dollari in *Bitcoin* per ripristinarli.

L'attacco ha causato interruzioni operative significative e sollevato preoccupazioni sulla sicurezza delle infrastrutture critiche. ENEL ha collaborato con le autorità e implementato misure di sicurezza aggiuntive per affrontare l'attacco. L'incidente evidenzia la necessità di una solida strategia di sicurezza informatica e di una cooperazione globale per contrastare le minacce cibernetiche e proteggere le infrastrutture critiche da futuri attacchi.

Successivamente, ENEL ha collaborato con le autorità competenti e ha implementato misure di sicurezza aggiuntive per affrontare l'attacco e mitigarne gli effetti. L'incidente ha evidenziato la necessità di avere una solida strategia di sicurezza informatica e di promuovere la cooperazione globale per contrastare le minacce cibernetiche e proteggere le infrastrutture critiche da futuri attacchi.

Classificazione generale dell'attacco
Numero di fasi
L'attacco con Netwalker coinvolge diverse fasi. Inizialmente, i cybercriminali si infiltrano nei sistemi informatici di ENEL, solitamente sfruttando

vulnerabilità o utilizzando tecniche di spear phishing per ottenere accesso non autorizzato o tramite un attacco RDP *brute force* derivato da *web server* vulnerabili (non configurati correttamente o non aggiornati). Successivamente, viene eseguita la criptazione dei file e viene inviata una richiesta di riscatto.
Velocità di attacco
Una volta che i cybercriminali hanno ottenuto accesso ai sistemi di ENEL, hanno criptato i file in modo rapido ed efficiente, causando danni immediati.
Tipologia di attacco
L'attacco con Netwalker è un attacco *ransomware*, che mira a criptare i file dell'azienda vittima e richiede un riscatto per ripristinarli. Questo tipo di attacco sfrutta tecniche di crittografia avanzate per rendere i file inaccessibili agli utenti legittimi.
Tipologia di attaccante
Netwalker, è stato identificato come un *ransomware-as-a-service* (RaaS), che significa che i cybercriminali vendono il *software* di Netwalker ad altri attaccanti, che a loro volta eseguono gli attacchi. In questo caso studio, dai dati raccolti, l'attacco pare sia attribuibile a un gruppo di hacker in lingua russa col nome di Circus Spider. Questo gruppo APT, basa le proprie azioni sull'ottenimento di risorse finanziarie mediante attacchi mirati ad aziende dei settori dell'educazione, dell'energia, governativi, della sanità, dell'industria e dei trasporti e logistica.
Obiettivo
L'obiettivo principale dell'attacco a ENEL con Netwalker era ottenere un riscatto finanziario. I cybercriminali cercavano di estorcere denaro all'azienda minacciando di pubblicare i dati criptati se il riscatto non veniva pagato. Il loro obiettivo era sfruttare l'importanza dei servizi forniti da ENEL nel settore energetico per aumentare la probabilità di pagamento del riscatto.
Risorse finanziarie

Gli attacchi ransomware richiedono risorse finanziarie per sviluppare e distribuire il *malware*. Inoltre, i cybercriminali richiedono un pagamento in criptovaluta come Bitcoin per il riscatto. Le dimensioni del riscatto possono variare a seconda dell'azienda vittima e della quantità di dati criptati.
Conseguenze
L'attacco a ENEL con Netwalker ha avuto conseguenze significative. Ha causato gravi interruzioni operative per l'azienda, portando a disagi per i clienti e possibili perdite finanziarie. Inoltre, l'incidente ha sollevato preoccupazioni sulla sicurezza delle infrastrutture critiche e sulla capacità degli attaccanti di colpire organizzazioni di importanza strategica.

Analisi della catena di attacco

Reconnaissance (Ricognizione):
Gli attaccanti hanno individuato una vulnerabilità o una falla nei sistemi di ENEL che permettesse loro di infiltrarsi. Ciò potrebbe essere avvenuto attraverso tecniche come il *phishing*, l'ingegneria sociale o *l'exploit* di vulnerabilità del software.
Weaponization (Armamento):
Il *payload* di Netwalker *ransomware* è il componente principale del *malware* che viene eseguito sul sistema infetto. Il suo obiettivo è crittografare i file dell'utente e richiedere un pagamento per ripristinarli. Il *payload* utilizza un algoritmo di crittografia, come Salsa20, per rendere i file illeggibili senza la chiave di decrittazione corretta. Successivamente, viene visualizzato un messaggio di richiesta di riscatto che spiega all'utente come effettuare il pagamento per ottenere la chiave di decrittazione. In alcuni casi, il *payload* può anche eseguire azioni distruttive, come cancellare le copie di backup o disabilitare la protezione del sistema. Tuttavia, pagare il riscatto non garantisce sempre il ripristino dei file, ed è sempre consigliabile prendere precauzioni per proteggere i dati e avere regolari *backup* dei file importanti.

Inoltre, sono stati aggiunti strumenti per il *deployement* (*toolkit*) che danno la possibilità agli attaccanti di trovare il metodo migliore di attacco. Contiene infatti una serie di tool all'interno che permettono all'attaccante di capire com'è l'architettura della rete, per fare escalation dei privilegi, strumenti per il supporto remoto e anche dei software per la rimozione degli antivirus. Proprio per questo motivo, è diventato molto più efficace ed efficiente.
Delivery (Consegna):
L'accesso iniziale pare sia avvenuto tramite Trickbot o Dridex, tipi di *malware* noti come *Trojan* bancari, progettati per rubare informazioni finanziarie sensibili come le credenziali di accesso ai conti bancari. Solitamente, questo avviene attraverso l'invio di e-mail di phishing contenenti allegati malevoli o *link* dannosi. Quando un utente apre l'allegato di una mail di Phishing o clicca su di un *link* malevolo, il malware viene scaricato e si installa sul computer dell'utente senza il suo consenso.
Exploitation (Sfruttamento):
Questo può includere la ricerca di informazioni pubbliche, come il rilevamento di indirizzi IP, nomi di dominio o informazioni sui dipendenti, nonché l'utilizzo di tecniche più avanzate come la scansione delle porte o l'analisi del traffico di rete. Una volta acquisita una conoscenza approfondita del sistema o della rete, gli attaccanti possono individuare le configurazioni errate o le debolezze nella sicurezza. Ciò potrebbe includere password deboli o facilmente indovinabili, errori di configurazione delle autorizzazioni di accesso, difetti nel sistema operativo o nelle applicazioni, o mancanza di patch di sicurezza aggiornate.
Installation (Installazione):
Il *ransomware* viene eseguito attraverso degli *script* PowerShell, detti offuscati, che contengono un'ampia porzione di dati codificati in Base64 su più livelli. Questo offuscamento non permette una facile e immediata lettura da parte degli addetti. Questi dati vengono decodificati e successivamente viene utilizzata

un’operazione di XOR per decifrare un *array* di *byte*. Infine, il *ransomware* carica la DLL principale in memoria per avviare l’esecuzione del processo di cifratura dei file. Questo tipo di minaccia sfrutta una tecnica chiamata *reflective dynamic-link library injection* (delle DLL), nota anche come *reflective DLL loading*. La tecnica consente l’iniezione di una DLL dalla memoria anziché dal disco. Questa tecnica è più stealth rispetto all’iniezione regolare di DLL perché, oltre a non avere bisogno del file DLL effettivo su disco, non ha bisogno di alcun processo di Windows per essere iniettato. Ciò elimina la necessità di registrare la DLL come modulo caricato di un processo e consente di sfuggire agli strumenti di monitoraggio del caricamento delle DLL. Il *payload* inizia con uno script *PowerShell* rilevato come Ransom.PS1.NETWALKER.B. Questo script verifica se il sistema colpito sia a 32 o 64 bit, quindi definisce quale DLL utilizzare che, successivamente, viene iniettata nel processo explorer.exe. Quindi il *ransomware* si attiva e vengono cancellate le copie nascoste del volume dati per evitare che la vittima le possa utilizzare per recuperare i propri file crittografati. La crittografia viene effettuata con Salsa20 e vengono aggiunte delle estensioni casuali ai file infettati. Salsa20 utilizza una chiave segreta di lunghezza fissa per generare un flusso di *byte* pseudocasuali, che vengono quindi utilizzati per crittografare i dati. L’algoritmo opera su blocchi di 64 byte alla volta e genera un flusso di *byte* di *output* della stessa lunghezza.

Per generare il flusso di *byte* pseudocasuali, Salsa20 utilizza una combinazione di operazioni di aritmetica modulare, operazioni di XOR e permutazioni dei dati. Ciò include l’applicazione di funzioni di round multiple su un vettore di stato interno, che viene poi combinato con i dati di input tramite l’operazione di XOR per produrre i *byte* di *output* crittografati.

Uno degli aspetti distintivi di Salsa20 è la sua resistenza alle attacchi di crittanalisi differenziale e lineare, il che significa che è considerato un algoritmo sicuro per l’uso nella crittografia di flusso. È stato progettato per essere veloce

e sicuro, ed è ampiamente utilizzato in diverse applicazioni, inclusi protocolli di comunicazione sicura e software di crittografia.
Command and Control (Comando e controllo):
Dopo che il malware è stato eseguito con successo sul sistema infetto, si connette a un server di comando e controllo remoto gestito dagli attaccanti. Questa connessione avviene attraverso il protocollo di rete, di solito tramite Internet, mediante l'utilizzo di indirizzi IP anonimi o compromessi, la crittografia delle comunicazioni e l'utilizzo di protocolli non standard, o reti di tipo botnet, consentendo agli aggressori di assumere il controllo del malware e delle azioni che esso compie sul sistema.
Actions on Objective (Azioni sull'obiettivo)
Queste azioni includono lasciare una nota di riscatto che informa le vittime della crittografia dei loro file e fornisce istruzioni per effettuare il pagamento del riscatto. Gli aggressori stabiliscono un canale di comunicazione per negoziare il pagamento e minacciano le vittime di perdere i dati crittografati. Viene richiesto un pagamento in criptovaluta, di solito Bitcoin, e gli aggressori possono fornire una dimostrazione di decifrazione per convincere le vittime. Si esercitano pressioni sulle vittime per accelerare il pagamento e, una volta ricevuto, gli aggressori monitorano attentamente il pagamento prima di fornire la chiave di decrittografia.

Conclusioni/Lezioni apprese
Gli attacchi ransomware di tipo Netwalker includono l'uso di tecniche avanzate di evasione, come il *ransomware fileless* e l'iniezione di DLL riflessiva. Questo ha dimostrato la capacità di evadere le tradizionali difese antivirus e anti-malware sfruttando il linguaggio di scripting come *PowerShell* per eseguire il codice direttamente in memoria, senza la necessità di salvare il file dannoso sul disco. Inoltre, ha fruttato la tecnica dell'iniezione di *dynamic-link library* (DLL) riflessiva per caricare il ransomware direttamente in memoria da un processo

legittimo, eludendo così la rilevazione. Queste tattiche rendono più difficile la rilevazione e la mitigazione dell'attacco, richiedendo soluzioni di sicurezza più avanzate per identificare e bloccare il *ransomware fileless*. È importante adottare soluzioni di sicurezza avanzate per rilevare e bloccare questi attacchi. Inoltre, è fondamentale avere regolari e aggiornati backup dei dati, consapevolezza degli utenti, monitoraggio e rilevamento tempestivo delle attività sospette. La collaborazione e la condivisione delle informazioni tra le organizzazioni sono essenziali per affrontare gli attacchi ransomware in modo efficace. La prevenzione, il monitoraggio costante e la prontezza a rispondere sono fondamentali per mitigare gli attacchi ransomware e ridurre i danni potenziali.

Fonti

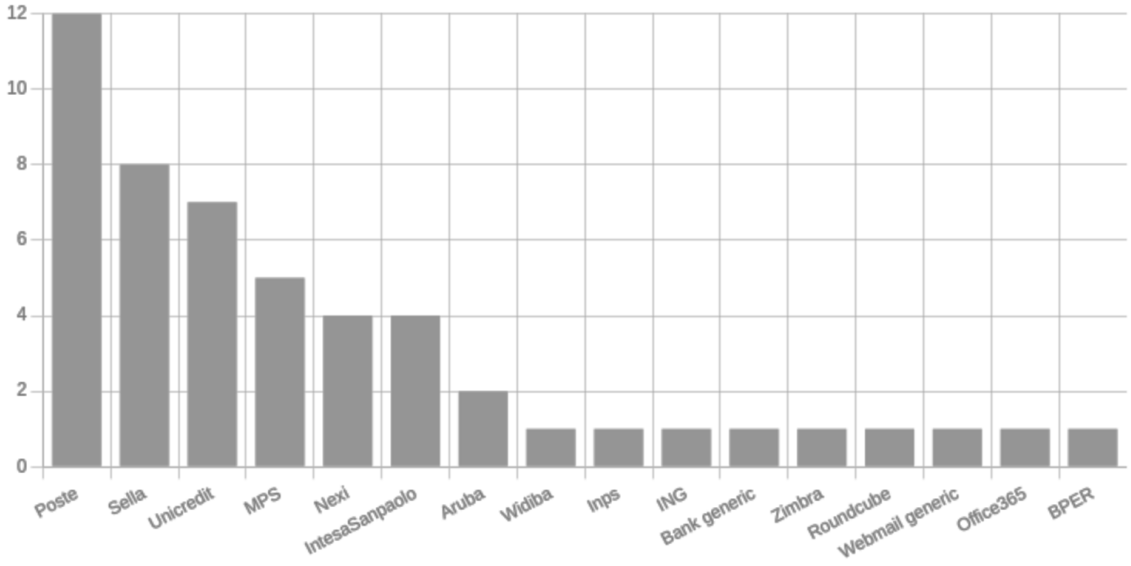
- CERT-AGID – Compute Emergency Response Team AGID, (2020), NetWalker: il ransomware che ha beffato l'intera community, https://cert-agid.gov.it/news/netwalker-il-ransomware-che-ha-beffato-lintera-community/
- Crowdstrike, (2020), Intelligence Report CSIT-20081 Technical analysis of the Netwlker ransomware, Crowdstrike global intelligence team.
- CSIRT, (2020), NetWalker Analisi di un ransomware, ACN – Agenzia per la Cybersicurezza Nazionale
- Ding, J., Qammar, A., Zhang, Z., Karim, A., & Ning, H. (2022). Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions. Energies, 15(18), 6799.
- ENEL, (2021), Risposta alle domande poste prima dell'Assemblea ai sensi dell'art. 127-ter del D. Lgs. n. 58/1998, Assemblea Ordinaria degli Azionisti di Enel S.p.A.
- ETDA Electronic Transactions Development Agency, (2022), APT group: Circus Spider
- FBI, Federal Bureau of Investigation – Cyber Division, (2020), FBI FLASH Alert number MI-000130-MW Indicators Associated with Netwalker Ransomware
- PCM-SISR (Presidenza del Consiglio dei Ministri – Sistema di Informazione per la Sicurezza della Repubblica, (2021), "Relazione sulla Politica dell'Informazione per la Sicurezza 2020"

- Wallis, T., Johnston, C., & Khamis, M. (2021). Interorganizational cooperation in supply chain cybersecurity: A cross-industry study of the effectiveness of the UK implementation of the NIS Directive. Information and Security: An International Journal, 48, 36-68.
- Zheng, T., Liu, M., Puthal, D., Yi, P., Wu, Y., & He, X. (2022). Smart Grid: Cyber Attacks, Critical Defense Approaches, and Digital Twin. arXiv preprint arXiv:2205.11783.

CAMPAGNE DI PHISHING ITALIANE

Le campagne di *phishing* in Italia sono diventate sempre più comuni e rappresentano una minaccia significativa per la sicurezza dei cittadini. Gli aggressori utilizzano tecniche di ingegneria sociale, mediante azioni ingannevoli, come l'invio di *e-mail* o messaggi di testo falsi, al fine di ottenere informazioni sensibili dai destinatari. Nella sola settimana dal 13 al 19 maggio, il CERT-AgID ha riscontrato e analizzato un totale di 62 campagne malevole nello scenario italiano. Di queste, 60 avevano come obiettivo specifico l'Italia, mentre due erano di natura generica ma coinvolgevano comunque il paese. Per quanto riguarda il phishing, sono state registrate 51 campagne, coinvolgendo 16 *brand*, principalmente nel settore bancario. Una campagna ha interessato in particolare 9 istituti bancari. Le attività di *smishing* nei confronti dell'INPS e il *phishing* generico mirato a ottenere credenziali di *webmail* sono continuate senza soluzione di continuità.

Tabella 8 - Phishing della settimana © 2023 CERT-AgID



Questi messaggi includono *link* a siti web falsi, che si fingono essere legittimi portali di corrieri, compagnie telefoniche, servizi energetici o servizi postali. Attraverso il *social engin*eering cercano di ingannare i visitatori, spingendo le vittime ad agire in modo tempestivo e a condividere le proprie credenziali di

accesso, informazioni personali o finanziarie e li convincono a scaricare il malware che infetta il loro computer. Inoltre, i domini utilizzati per questi siti di phishing vengono generati e disabilitati dopo un breve periodo di tempo. A volte vengono utilizzate anche le tecniche di *typosquatting* che consistono nel presentare un link di connessione malevolo sfruttando gli errori di digitazione commessi dagli utenti durante l'inserimento di un indirizzo web. Consiste nel registrare nomi di dominio simili a quelli di siti web legittimi, ma con piccole variazioni come errori di ortografia, scambi di lettere o l'aggiunta di caratteri extra. L'obiettivo è ingannare gli utenti e indurli a visitare questi siti falsi, che spesso cercano di raccogliere informazioni personali o diffondere malware. Ad esempio, un aggressore potrebbe registrare un dominio come "goggle.com" anziché "google.com", contando sul fatto che gli utenti potrebbero commettere errori di digitazione e finire per visitare il sito malevolo.

L'obiettivo principale di queste campagne di *phishing* è sfruttare la fiducia delle persone verso istituzioni legittime al fine di ottenere accesso non autorizzato ai loro account o di commettere frodi finanziarie. Gli aggressori cercano di creare un senso di urgenza o paura nei destinatari, spingendoli a fornire informazioni sensibili senza pensarci due volte.

Gli attacchi possono sfruttare diversi vettori, tra cui siti web, email e reti sociali online (OSN), così come SMS, chiamate automatizzate e malware (figura 14). Pertanto, le tecniche di difesa utilizzano un ampio insieme di diverse caratteristiche per individuare possibili attacchi. Gli attacchi di *phishing* possono essere perpetrati per una vasta gamma di obiettivi maligni, come il furto di informazioni sensibili e frodi finanziarie. Questa diversità di obiettivi e tecniche pone sfide nella rilevazione degli attacchi di *phishing*.

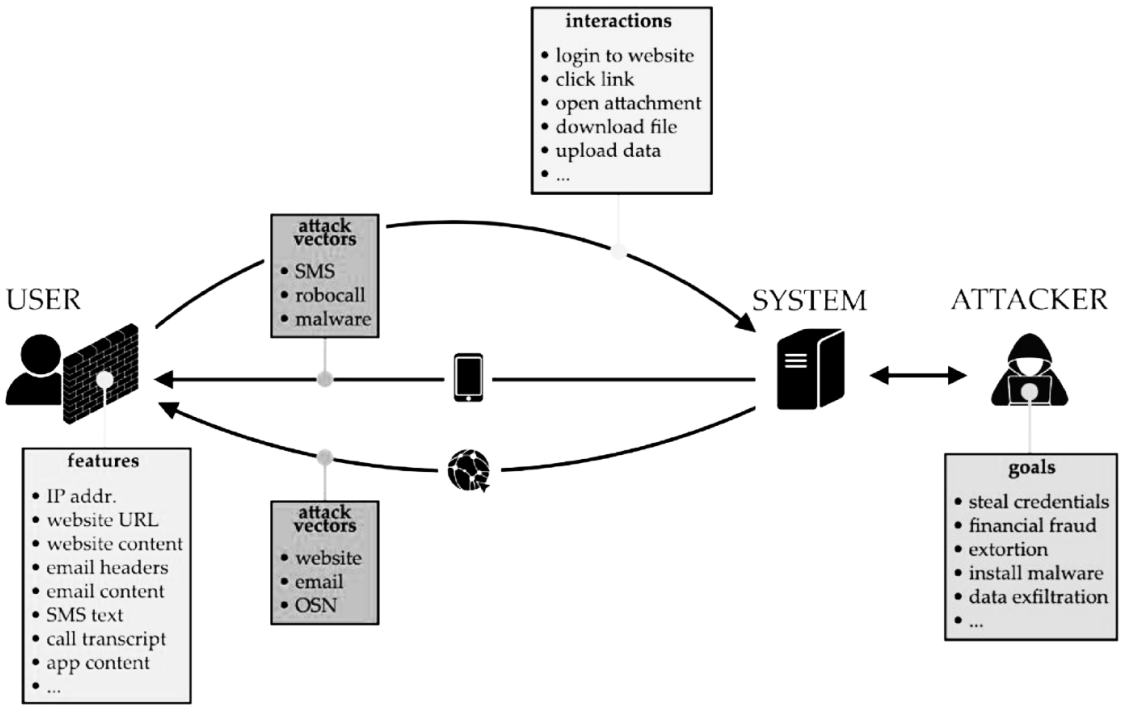


Figura 14 - Complessità e dimensioni degli attacchi di phishing © 2022, AL-QAHTANI AND CRESCI

Classificazione generale dell'attacco
Numero di fasi
Le campagne di *phishing* coinvolgono solitamente diverse fasi. Queste includono la pianificazione e la preparazione dell'attacco, la creazione di messaggi di *phishing* ingannevoli, l'invio di tali messaggi agli obiettivi selezionati, l'acquisizione delle informazioni personali o finanziarie delle vittime e l'utilizzo di tali informazioni per scopi fraudolenti. Struttura di un attacco di phishing in tre fasi: 1. Creazione di un sito web falso che imita il sito web della banca che è l'obiettivo dell'attacco... 2 Caricamento della pagina sul proprio sito o compromissione di un sito esistente...

3 Invio di email di massa per attirare gli incauti verso il sito falso... La combinazione di questi tre elementi consente all'attaccante di effettuare un attacco. Il successo dell'attacco dipende da molti fattori, come la credibilità del sito, il contenuto del messaggio email e altri fattori, sia lato attaccante sia lato della vittima.
Velocità di attacco
Possono essere scagliate in modo massivo e rapido, con l'invio di un gran numero di e-mail o messaggi di testo in un breve lasso di tempo. Questa velocità permette agli aggressori di raggiungere un ampio pubblico e di aumentare le probabilità di successo dell'attacco.
Tipologia di attacco
Sono generalmente classificate come attacchi di ingegneria sociale, in cui gli aggressori cercano di manipolare le persone e indurle a rivelare informazioni sensibili o a compiere azioni non sicure. Le tecniche comuni includono l'invio di e-mail o messaggi di testo falsi, la creazione di siti web fraudolenti che imitano quelli legittimi delle istituzioni finanziarie o governative e l'utilizzo di messaggi persuasivi per indurre le vittime a compiere determinate azioni. Nel periodo di osservazione del CERT-AgID, le campagne malevole si sono basate su 11 temi diversi per veicolare gli attacchi in Italia. Ecco i principali temi rilevati: **Banking**: utilizzato principalmente per campagne di phishing e smishing rivolte ai clienti di banche italiane, al fine di compromettere dispositivi Android attraverso il malware Brata e il malware Snake Keylogger. **Ordine**: sfruttato per diffondere i *malware* Formbook, Avemaria, Remcos e AgentTesla. **Avvisi sicurezza**: argomento utilizzato per le campagne di phishing mirate a ottenere credenziali di *webmail*. Un'ulteriore minaccia è costituita dal *phishing* adattivo.

In passato, i loghi e i marchi utilizzati nelle campagne di phishing erano predeterminati dagli autori prima dell'avvio della campagna. Tuttavia, l'evoluzione delle tecniche di *phishing* ha portato all'uso di contenuto dinamico, che si adatta alla vittima in base al suo dominio. Ciò significa che gli autori di queste campagne di phishing non creano campagne diverse per ogni organizzazione da colpire, ma piuttosto utilizzano modelli e contenuti che vengono personalizzati automaticamente in base al dominio dell'organizzazione vittima. Questo approccio mira ad aumentare l'efficacia dell'attacco, rendendo le email e le pagine di *phishing* più convincenti e credibili per le vittime. L'utilizzo di contenuto dinamico può includere elementi come il logo dell'organizzazione vittima, l'aspetto grafico del sito web o le informazioni specifiche dell'utente. Ciò rende le campagne di *phishing* più sofisticate e difficili da riconoscere per le persone non esperte. Infine, la nuova minaccia definita dal CSIRT-ITA "*Phishing-as-a-service*" per permettere anche ai meno esperti di condurre campagne finalizzate al furto di dati e credenziali degli utenti.
Tipologia di attaccante
Gli attaccanti possono essere individui o gruppi di cybercriminali. Possono essere organizzazioni criminali che mirano a ottenere profitti finanziari attraverso frodi o estorsioni.
Obiettivo
L'obiettivo è generalmente quello di ottenere informazioni finanziarie sensibili, come le credenziali di accesso ai conti bancari o i dati delle carte di credito. Gli aggressori possono utilizzare queste informazioni per effettuare frodi finanziarie o per accedere ai conti bancari delle vittime.
Risorse finanziarie
Le campagne di phishing richiedono una certa pianificazione e risorse per essere eseguite con successo. Gli aggressori possono investire tempo e denaro per

creare siti web e messaggi convincenti, nonché per orchestrare l'invio massivo di e-mail o messaggi di testo.
Conseguenze
Le conseguenze delle campagne di *phishing* possono essere gravi per le vittime e per le istituzioni coinvolte. Le vittime possono subire danni finanziari, perdere l'accesso ai propri account bancari o subire furto di identità. Le istituzioni coinvolte possono incorrere in danni reputazionali e legali a seguito di violazioni della sicurezza dei dati dei propri clienti.

Analisi della catena di attacco

Reconnaissance (Ricognizione):
Gli aggressori conducono ricerche per identificare potenziali obiettivi e sviluppano un piano per la campagna di phishing. Questo può includere la scelta di vittime specifiche, l'identificazione di temi o contenuti persuasivi e la selezione di tecniche di ingegneria sociale. In caso di attacchi mirati, questa fase può prevedere anche vere e proprie operazioni di Ingegneria sociale (SE). Gli attaccanti conducono quindi una ricerca preliminare per identificare potenziali vittime e ottenere informazioni sulle loro abitudini online e le vulnerabilità. Quindi, nella fase iniziale dell'attacco di ingegneria sociale, l'attaccante stabilisce gli obiettivi specifici dell'attacco, come il furto di credenziali o l'ottenimento di informazioni sensibili, e identifica i potenziali obiettivi di interesse. Successivamente, l'attaccante raccoglie informazioni contestuali aggiuntive, spesso provenienti da fonti aperte ed esterne, per affinare la lista degli obiettivi. Questa fase di ricognizione e *intelligence* delle fonti aperte (OSINT) consente all'attaccante di migliorare la pianificazione dell'attacco, inclusa l'aggiunta di nuovi obiettivi scoperti o l'individuazione di obiettivi intermedi che possono essere sfruttati per raggiungere l'obiettivo finale, come infiltrarsi nella gerarchia di un'organizzazione.

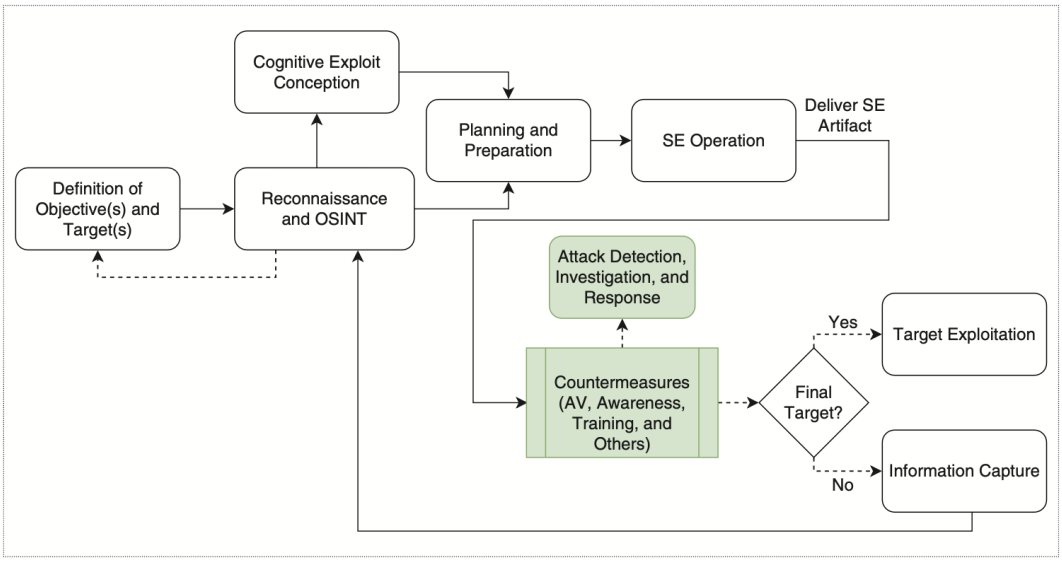


Figura 15 - Lo schema delle fasi degli attacchi di ingegneria sociale e il ruolo delle contromisure © 2019 Allodi

Diversamente, nel caso di attacchi massivi, sono spesso condotti in modo indiscriminato, mirando a un vasto numero di potenziali vittime utilizzando email o altre forme di interazione sociale. Gli attaccanti sviluppano sia il messaggio di *phishing* che il *payload* dannoso da consegnare alle vittime. Le caratteristiche cognitive come la scarsità, la prova sociale, il gradimento e l'autorità vengono sfruttate per aumentare le probabilità di successo dell'attacco. Le vittime di *phishing* sono generalmente selezionate da dati trapelati o rubati da specifici settori o servizi, ma gli attacchi di phishing generici non sono personalizzati per un profilo specifico di vittima, ma mirano a un pubblico più ampio e variegato.

Weaponization (Armamento):

Gli aggressori creano e-mail o messaggi di testo che sembrano provenire da fonti legittime, come banche, aziende o servizi online. Utilizzano tecniche di *spoofing* per falsificare l'indirizzo del mittente e creare un aspetto autentico.

Gli attaccanti mettono in atto diverse strategie per rendere i loro contenuti credibili e convincenti. Ad esempio, possono creare email che sembrano provenire da istituti finanziari o servizi online popolari, utilizzando loghi, grafica

e testo simile a quelli ufficiali. Possono anche creare siti web falsi che imitano l'aspetto e la struttura di siti legittimi, al fine di ingannare le vittime e far loro condividere informazioni personali o effettuare transazioni finanziarie. L'obiettivo principale della *weaponization* è rendere i mezzi di attacco il più convincenti possibile, al fine di aumentare le probabilità di successo dell'attacco di phishing. È importante sottolineare che la predisposizione non si limita solo all'aspetto tecnico della creazione di contenuti dannosi, ma coinvolge anche la pianificazione strategica di come utilizzare tali contenuti nel contesto dell'attacco di *phishing*. Gli attaccanti cercano di massimizzare l'impatto e la diffusione dei loro mezzi di attacco, adottando tattiche mirate e adattando i contenuti alle caratteristiche delle vittime e al contesto in cui operano.
Delivery (Consegna):
Le e-mail di *phishing* vengono inviate alle vittime attraverso diverse modalità, come l'invio di massa o l'indirizzamento mirato. Gli aggressori possono utilizzare *botnet*, *server* compromessi o altri mezzi per distribuire le e-mail in modo efficace.
Exploitation (Sfruttamento):
Le vittime vengono indotte a interagire con l'e-mail di *phishing* attraverso l'uso di tattiche persuasive. Questo può includere richieste di azioni immediate, minacce o offerte allettanti. Inoltre, vengono ingannate per fornire informazioni sensibili o compiere azioni indesiderate. Gli aggressori utilizzano tecniche di ingegneria sociale per manipolare le vittime, ad esempio facendo leva sulla paura, la curiosità o l'urgenza. Nel 2020, in piena pandemia, una campagna di false email, apparentemente provenienti da un centro medico e redatte in lingua giapponese, con il pretesto di fornire aggiornamenti sulla diffusione del virus, invitavano ad aprire un allegato malevolo che mirava ad impossessarsi delle credenziali bancarie e dei dati personali della vittima. Nel 2021 invece, alcune mail di istituti di credito

facevano leva su di una presunta partnership con la Polizia Postale. Questo andava a incrementare le possibilità di successo nell'apertura dell'allegato contenente contenuto malevolo. Nel 2022, lo scopo dell'autore di una mail consisteva nella richiesta di un pagamento in *Bitcoin* per scongiurare la pubblicazione di dati aziendali sensibili di cui il malfattore sarebbe stato in possesso. Altre minacce interessavano pacchi in giacenza, fantomatici cacciatori di teste interessati ai profili professionali delle vittime, fino, nel 2023, a richieste di ripristino delle proprie credenziali in concomitanza con l'episodio di indisponibilità dei servizi erogati da Virgilio e Libero.
Installation (Installazione):
Avviene generalmente tramite l'invio di messaggi di *phishing* contenenti link malevoli o allegati infetti, che una volta aperti o cliccati dall'utente, consentono all'attaccante di installare *malware* sul sistema della vittima. Questi possono comprendere siti web fittizi, SMS, chiamate telefoniche, pagine e *account social media* falsi, app malevoli.
Command and Control (Comando e controllo):
Gli aggressori cercano di ottenere le credenziali di accesso delle vittime, ad esempio *username* e *password*, attraverso l'uso di pagine di *login* contraffatte o *link* malevoli che indirizzano le vittime a siti web falsi. Quindi cercano di mantenere l'accesso al sistema o *all'account* delle vittime a lungo termine, ad esempio attraverso il *download* di *malware* o l'installazione di *backdoor*.
Actions on Objective (Azioni sull'obiettivo)
Gli obiettivi degli attaccanti possono variare a seconda delle loro intenzioni. Nel caso in cui l'obiettivo sia l'installazione di un *software* specifico sul computer della vittima, gli attaccanti possono utilizzare diverse tecniche, come l'invio di file eseguibili dannosi o l'induzione della vittima a scaricare e installare *software* compromessi. Una volta installato, il *software* dannoso potrebbe consentire agli

attaccanti di eseguire azioni non autorizzate sul sistema o di ottenere informazioni riservate.
D'altra parte, se l'obiettivo degli attaccanti è il furto di identità, esistono diverse modalità per raggiungere questo scopo. Una di queste è l'ingegneria sociale, in cui gli attaccanti creano pagine web false o cloni di siti legittimi al fine di indurre la vittima a inserire le proprie credenziali, che vengono poi registrate e utilizzate dagli attaccanti per scopi fraudolenti.
Inoltre, i *keylogger* sono una categoria di software progettati per registrare tutte le tastate effettuate dalla vittima sulla tastiera del PC. Gli attaccanti possono utilizzare *keylogger* per catturare informazioni sensibili, come username, *password*, numeri di carte di credito o altre informazioni personali. I dati registrati vengono quindi inviati all'attaccante, consentendo loro di accedere all'account e alle informazioni personali della vittima.

Le credenziali raccolte vengono utilizzate per accedere a sistemi o account legittimi delle vittime. Gli aggressori possono rubare informazioni sensibili, installare *malware* o compiere altre azioni dannose.
Inoltre, sfruttano le informazioni raccolte o l'accesso ottenuto per fini illeciti, ad esempio rubando denaro, vendendo informazioni sensibili o utilizzando le vittime per ulteriori attacchi.

Conclusioni/Lezioni apprese
Seppur nel corso del 2022, la Polizia sia riuscita a identificare e indagare 853 persone (+9% rispetto l'anno precedente) in merito a campagne di *phishing*, *smishing* e *vishing* al fine di carpire illecitamente dati personali e bancari, vi sono delle attività di prevenzione che possono portare ad aumentare il livello di attenzione situazionale. Al primo posto vi è la necessità di consapevolezza e formazione degli utenti per riconoscere le tecniche di phishing e adottare pratiche sicure.

Le organizzazioni devono implementare misure di sicurezza avanzate, come soluzioni *anti-phishing* e filtri email, e monitorare costantemente gli eventi di phishing per rispondere tempestivamente agli attacchi.
La condivisione delle informazioni tra organizzazioni e la collaborazione con forze dell'ordine ed esperti di sicurezza informatica sono fondamentali.
È importante mantenere il *software* aggiornato con gli ultimi aggiornamenti di sicurezza e monitorare attentamente le transazioni finanziarie per rilevare attività sospette.
Gli attacchi di *phishing* sono in continua evoluzione, quindi le strategie di sicurezza devono essere adattate costantemente.
In definitiva, la prevenzione e la risposta efficace agli attacchi di *phishing* richiedono un approccio olistico che coinvolge la consapevolezza degli utenti, la tecnologia avanzata e la collaborazione tra le parti interessate.

Per proteggersi dal *phishing*, è importante adottare le seguenti misure di sicurezza:
1. **Verifica dell'attendibilità**: Assicurarsi sempre dell'attendibilità del soggetto con cui si comunica. Richiedere e verificare l'indirizzo email aziendale o il contatto telefonico dell'azienda per confermare l'autenticità delle comunicazioni ricevute.
2. **Blocco dell'esecuzione di software non attendibile e non firmato**: Evitare di eseguire o aprire software proveniente da fonti non attendibili o non firmato digitalmente. Questo aiuta a ridurre il rischio di eseguire malware o software dannoso.
3. **Aggiornamento dei software di sicurezza**: Mantenere sempre aggiornati i *software antivirus*, *anti-malware* e i sistemi endpoint. Gli aggiornamenti regolari includono nuove definizioni di virus e patch di sicurezza che proteggono dai nuovi tipi di minacce.

4. **Prudenza nell'aprire file eseguibili**: Non avviare file eseguibili a meno che non si sia certi della loro provenienza e legittimità. Eseguire solo file provenienti da fonti affidabili e verificate.

5. **Analizzare la sintassi:** delle frasi, l'ortografia delle parole e l'impostazione grafica. Spesso dietro questi elementi si cela una mail di *phishing*.

Inoltre, è consigliabile adottare le seguenti buone pratiche di sicurezza informatica:

- Utilizzare *password* complesse e uniche per gli *account online* e cambiarle periodicamente.
- Evitare di cliccare su link sospetti o allegati di email provenienti da mittenti sconosciuti o non attendibili.
- Mantenere il sistema operativo e le applicazioni sempre aggiornate con le ultime patch di sicurezza.
- Fare regolarmente il *backup* dei dati importanti su dispositivi di archiviazione esterni o su cloud sicuri.
- Utilizzare una connessione *Internet* sicura e crittografata quando si accede a informazioni sensibili o si effettuano transazioni online.
- Essere consapevoli delle tattiche di *social engineering*, come l'ingegneria sociale via telefono o email, e adottare misure di cautela.
- Educare se stessi e gli utenti sull'importanza della sicurezza informatica e su come riconoscere le minacce online.

Fonti

- ACN, (2022), Nota-stampa-CSIR-Italia-attenti-alle-truffe.pdf
- ACN, (2022), Scam: campagna di phishing a tema corrispondenza (BL01/221124/CSIRT-ITA)
- ACN, (2023), Campagna di smishing sfrutta il recente down dei servizi Libero e Virgilio
- AGID CERT-PA, (2018), phishing cos'è e come evitarlo

- AGID CERT-PA, (2021), In crescita il fenomeno delle campagne di phishing adattivo
- AGID CERT, (2023), Sintesi riepilogativa delle campagne malevole nella settimana del 13 – 19 maggio 2023 – CERT-AGID
- Al-Qahtani, A. F. and Cresci, S. (2022) "The Covid-19 Scamdemic: A Survey of Phishing Attacks and Their Countermeasures during Covid-19," IET Information Security, 16(5), pp. 324–345. doi: 10.1049/ise2.12073.
- Allodi L., Chotza T., Panina E. and Zannone N., (2020), "The Need for New Antiphishing Measures Against Spear-Phishing Attacks," in IEEE Security & Privacy, vol. 18, no. 2, pp. 23-34, March-April 2020, doi: 10.1109/MSEC.2019.2940952.
- Baldoni, R., De Nicola, R., Prinetto, P. E., Anglano, C. F., Aniello, L., Antinori, A., ... & Zanero, S. (2018). Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici.
- Caviglia, F., Cerulli, M., Davidzon, I., & Delfino, M. (2009). Spam e phishing. Se le conosci, le eviti. A. Andronico, L. Colazzo (a cura di), Didamatica.
- CSIRT Italia, (2020), Phishing as a Service Framework, CERT.LV
- Forte, D. (2009). Anatomy of a phishing attack: a high-level overview. Network Security, 2009(4), 17-19.
- Gutierrez, C. N., Kim, T., Della Corte, R., Avery, J., Goldwasser, D., Cinque, M., & Bagchi, S. (2018). Learning from the ones that got away: Detecting new forms of phishing attacks. IEEE Transactions on Dependable and Secure Computing, 15(6), 988-1001.
- Polizia di Stato Phishing, (2020), le truffe informatiche legate al Coronavirus
- Polizia di Stato Phishing, (2021), I cybertruffatori sfruttano il nome della Polizia postale
- Polizia di Stato, (2023), I dati 2022 della Polizia postale.
- Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., ... & Bursztein, E. (2017, October). Data breaches, phishing, or malware? Understanding the risks of stolen credentials. In Proceedings of the 2017 ACM SIGSAC conference on computer and communications security (pp. 1421-1434).

CAPITOLO 7 – CONCLUSIONI

Le analisi svolte nel contesto di questa tesi hanno esaminato le azioni di *Cyber Warfare*, concentrandosi sui rischi attuali e sulle minacce future ai sistemi informatici. Attraverso un'analisi dettagliata dell'ambiente cibernetico, delle minacce e dei rischi ad esso associati, nonché degli attori coinvolti e delle difese disponibili, abbiamo acquisito una visione completa delle sfide che il contesto della *Cyber Warfare* presenta.

Secondo il report sul futuro della Cybersecurity in Italia (Baldoni, 2018), *la digitalizzazione della vita umana presenta sia opportunità che minacce*. Il report sostiene che oltre alle campagne di *ransomware* come WannaCry, il *phishing* e le *fake news*, esistono molte altre minacce nel contesto della trasformazione digitale. Questi esempi, rappresentano solo la punta dell'iceberg, mentre al di sotto di essa si verificano quotidianamente migliaia di campagne di attacchi mirati o diffusi su larga scala, condotte da stati sovrani, cybercriminali e attivisti politici. Questi attacchi mirano a colpire infrastrutture critiche, aziende, istituzioni governative e cittadini con l'obiettivo di rubare dati, monitorare comportamenti, assumere il controllo dei sistemi operativi e perpetrare truffe. È fondamentale comprendere che le minacce digitali vanno al di là delle manifestazioni più evidenti e richiedono una costante attenzione e protezione da parte di tutti gli attori coinvolti.

L'esplorazione dell'ambiente operativo ha permesso di evidenziarne la complessità e l'importanza crescente nella società odierna. In effetti, esso richiede una visione olistica che comprenda anche la sicurezza informatica e la gestione dei rischi nel ciberspazio, riconoscendo che le vulnerabilità e le minacce cibernetiche possono avere effetti profondi e diffusi in qualsiasi dimensione dell'ambiente operativo.

Proprio per questo motivo, nell'era del dato e dell'informazione, la *Cyber Warfare* rappresenta una delle principali sfide per la sicurezza nazionale e internazionale, nonché una delle maggiori minacce alla sicurezza globale. Una visione olistica dell'ambiente operativo deve quindi comprendere necessariamente la gestione delle minacce cibernetiche e la difesa del ciberspazio, riconoscendo l'importanza di questa componente per la sicurezza globale

Una delle peculiarità della *Cyber Warfare* è che può essere condotta in modo anonimo e remoto, il che la rende un'arma attraente per i paesi che cercano di esercitare influenza a livello globale. La crescente minaccia della *Cyber Warfare* alla sicurezza sia internazionale che nazionale, richiede una risposta coesa e unificata da parte di tutti gli attori coinvolti. L'approccio integrato alla gestione dei rischi, la cooperazione a livello nazionale e internazionale e la sensibilizzazione sulla sicurezza informatica si rivelano essenziali per contrastare le minacce della Cyber Warfare e proteggere l'ambiente operativo. (NATO Cyber Defence Centre of Excellence, 2021; Relazione Annuale DIS, 2022).

Nel corso della ricerca, sono state esplorate le varie tipologie di minacce cibernetiche, ognuna con obiettivi specifici e modalità di attuazione, e gli impatti che possono generare sui sistemi informatici, sui sistemi industriali e aziendali. Lo scopo di queste consiste nella compromissione della sicurezza dei sistemi informatici al fine di ottenere informazioni o causare danni. Inoltre, si traducono in scenari di rischio che denotano complessità, nonché vastità delle azioni, delle operazioni e del potenziale conflitto *cyber*. A questo proposito, sono state analizzate le principali categorie di attacchi *cyber* che, in alcuni casi, possono anche trasformarsi in attacchi fisici o cinetici, ovvero gli attacchi cinetici alle Infrastrutture Critiche. Dietro l'attuazione di una minaccia, l'esecuzione di un attacco o lo sfruttamento di una vulnerabilità, i nostri studi ci hanno portato ad indagare gli attori coinvolti nella *Cyber Warfare,* dagli stati sovrani ai gruppi di cybercriminali dagli attivisti politici e agli *hacker*, analizzando nel dettaglio come

ogni categoria operi secondo finalità e obiettivi differenti pur sfruttando le medesime tecniche, tattiche e procedure.

Successivamente, la nostra analisi ha esplorato le difese disponibili per proteggere i sistemi informatici dagli attacchi. Abbiamo esaminato le strategie di *cybersecurity*, sia da un punto di vista di prevenzione che di reazione. Quindi, attraverso l'applicazione del modello di analisi degli incidenti organizzativi, è stato possibile studiare le principali azioni interne ed esterne e gli elementi peculiari fisici e metodologici che possono concorrere al sistema di difesa, ovvero di poter far fronte alla crescente minaccia cibernetica. Tuttavia, abbiamo riconosciuto che le difese devono continuamente adattarsi alle nuove minacce e rimanere all'avanguardia per garantire un'efficace protezione.

Quindi, in tema di sfide e prospettive future della *Cyber Warfare* abbiamo sottolineato l'importanza di una collaborazione internazionale nel contrastare le minacce, l'urgente necessità di sviluppare tecnologie innovative e politiche di *cybersecurity* avanzate. Inoltre, poiché l'evoluzione tecnologica e l'interconnessione sempre più diffusa delle reti e dei dispositivi informatici e fisici (IoT) comportano nuovi rischi e minacce, è necessario adottare nuove architetture, approcci e strategie di protezione che possano includere anche l'intelligenza artificiale (AI), la sensibilizzazione e la formazione continua di professionisti della sicurezza, elementi tutti fondamentali per creare una cultura della sicurezza e poter ridurre il rischio degli attacchi basati sugli errori umani e sulla non comprensione della situazione. Infine, risulterà determinante promulgare leggi e normative specifiche atte a contrastare gli scenari che si prospetteranno nei prossimi anni.
Affrontare queste sfide future richiederà un impegno costante nella ricerca, nell'innovazione e nella collaborazione tra enti pubblici e privati. Anticipare e prepararsi in vista delle minacce emergenti sarà cruciale al fine di mantenere la sicurezza nell'era digitale e proteggere le reti e le informazioni vitali per la società.

Attraverso lo studio di casi di studio significativi occorsi in Italia e all'estero è stato possibile evidenziare la complessità e l'impatto reale delle azioni di Cyber Warfare, offrendo spunti preziosi per comprendere le dinamiche degli attacchi e le loro implicazioni.

In conclusione, la nostra ricerca ha messo in luce l'urgente necessità di affrontare le minacce e i rischi della *Cyber Warfare* in modo tempestivo ed efficace. Gli sviluppi tecnologici, insieme all'evoluzione delle tattiche e delle strategie degli attaccanti, richiedono un costante adattamento delle difese e una maggiore consapevolezza delle implicazioni legate alla sicurezza informatica.
La *Cyber Warfare* rappresenta una minaccia in costante evoluzione per i sistemi informatici. Solo attraverso un approccio integrato, la cooperazione internazionale, lo scambio di informazioni, la condivisione delle migliori pratiche tra i paesi e l'adozione di soluzioni innovative, possiamo affrontare le sfide attuali e future e proteggere la sicurezza e la stabilità nel contesto digitale. La prevenzione degli attacchi informatici deve rimanere una priorità globale, in modo da garantire la sicurezza nazionale e internazionale. Solo attraverso uno sforzo collettivo sarà possibile contrastare in modo efficace la *Cyber Warfare* e garantire la sicurezza dei sistemi informatici su scala globale.

In definitiva, la *Cyber Warfare* rappresenta una minaccia complessa, in continua evoluzione per i sistemi informatici e per gli esseri umani. Affrontare efficacemente questa minaccia richiede una visione olistica, un impegno costante nella ricerca e nell'innovazione al fine di proteggere l'integrità e la sicurezza dei sistemi informatici. Solo attraverso una risposta coordinata e multidisciplinare, basata sulla prevenzione, la collaborazione e l'innovazione, sarà possibile affrontare le sfide attuali e future, proteggendo la sicurezza e la stabilità nel contesto digitale.

Bibliografia

LIBRI

- Andress J., Winterfeld Steve, (2014), Cyber Warfare (Second Edition), Chapter 12 - Non-State Actors in Computer Network Operations, Editor(s): Jason Andress, Steve Winterfeld, Syngress, Pages 207-219.
- Clusit Community for Security, (2022), SUPPLY CHAIN SECURITY L'importanza di conoscere e gestire i rischi della catena di fornitura, Supply Chain Security
- Farina F., Marrocco M, (2018). Complessità di security e gestione del rischio. Il modello a «misurazione continua dell'efficacia», Roma, Themis Edizioni, p.51
- Franchina L., Lucariello A., (2018), Governare il cyber risk. Una guida per amministratori e sindaci, Roma, Themis Edizioni, pp.35-38, 47-56
- Hadnagy, C. (2010). Social Engineering: The Art of Human Hacking. Wiley
- Hagestad II. William T. 2012. 21st Century Chinese Cyberwarfare. An examination of the Chinese cyberthreat from fundamentals of Communist policy regarding information warfare through the broad range of military, civilian and commercially supported cyberattack threat vectors. Cambridgeshire, UK: IT Governance Publishing.
- Hawkins, F. H., & Orlady, H. W. (1993). Human Factors in Flight (2nd ed.). Ashgate.
- Lapi M. (2021), Open Source Intelligence, Metodologie e strumenti per investigare il web, Edizioni Themis, Roma
- Perlroth, N. (2021). This Is How They Tell Me the World Ends: The Cyberweapons Arms Race. Bloomsbury Publishing
- Salini C. Brando G. Di Costanzo M., (2023) Il ransomware nell'economia del cybercrime. Analisi d'intelligence sul gruppo Conti, Themis Edizioni, Roma
- Stallings, W., & Brown, L. (2015). Computer Security: Principles and Practice (3rd). Pearson
- Teti, A (2021), Spycraft Revolution. Spionaggio e servizi segreti nel terzo millennio, Catanzaro: Rubbettino Editore. Pag.92
- Teti, A. (2018). Cyber Espionage e Cyber Counterintelligence. Spionaggio e controspionaggio cibernetico. Catanzaro: Rubbettino Editore.

PUBBLICAZIONI

- (BL01/221124/CSIRT-ITA)
- ACN, (2022), Nota-stampa-CSIR-Italia-attenti-alle-truffe.pdf
- ACN, (2022), Scam: campagna di phishing a tema corrispondenza
- ACN, (2023), Campagna di smishing sfrutta il recente down dei servizi Libero e Virgilio
- AGID CERT-PA, (2018), phishing cos'è e come evitarlo
- AGID CERT-PA, (2021), In crescita il fenomeno delle campagne di phishing adattivo
- AGID CERT, (2023), Sintesi riepilogativa delle campagne malevole nella settimana del 13 – 19 maggio 2023 – CERT-AGID
- Akbanov, M., Vassilakis, V. G., & Logothetis, M. D. (2019). WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. Journal of Telecommunications and Information Technology, (1), 113-124.
- Al-Qahtani, A. F. and Cresci, S. (2022) "The Covid-19 Scamdemic: A Survey of Phishing Attacks and Their Countermeasures during Covid-19," IET Information Security, 16(5), pp. 324–345. doi: 10.1049/ise2.12073.
- Arwood, S., Mills, R. & Raines, R., (2010), Operational art and Strategy in Cyberspace, Academic Conferences International Limited, Reading.
- Assante, M. J. (2016). Confirmation of a coordinated attack on the Ukrainian power grid. SANS Industrial Control Systems Security Blog, 207.
- Badhwar, R. (2021) The ciso's next frontier : ai, post-quantum cryptography and advanced security paradigms. Cham: Springer. doi: 10.1007/978-3-030-75354-2.
- Baezner, M., & Robin, P. (2017). Stuxnet (No. 4). ETH Zurich.
- Baldoni, R., De Nicola, R., Prinetto, P. E., Anglano, C. F., Aniello, L., Antinori, A., ... & Zanero, S. (2018). Il Futuro della Cybersecurity in Italia: Ambiti Progettuali Strategici.
- Bengt G. (2017), Securing Industrial Control Systems. SANS Institute, Nozomi Network
- Benjamin, M. (2013). Drone Warfare: Killing by Remote Control. Verso.
- Bissell K., LaSalle R., Dal Cin P.(2019). Ninth annual cost of cybercrime study. Accenture.

- Brambilla (Assiteca Sicurezza Informatica), (2017), Vademecum WannaCry: cos'è e come proteggersi https://www.assiteca.it/wp-content/uploads/2017/05/WannaCry-VADEMECUM-15.05.17.pdf
- Brundage, M. et al. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. ArXiv, abs/1802.07228.
- Calzarossa, Maria Carla & Lotto, I. & Rogerson, Simon. (2010). Ethics and information systems — Guest editors' introduction. Information Systems Frontiers. 12. 357-359. 10.1007/s10796-009-9198-4.
- Case, D. U. (2016). Analysis of the cyber attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC), 388, 1-29.
- Caviglia, F., Cerulli, M., Davidzon, I., & Delfino, M. (2009). Spam e phishing. Se le conosci, le eviti. A. Andronico, L. Colazzo (a cura di), Didamatica.
- Centre for Cybersecurity (CFCS) of Denmark, (2021), SolarWinds: State-sponsored global software supply chain attack,
- CERT-AGID – Compute Emergency Response Team AGID, (2020), NetWalker: il ransomware che ha beffato l'intera community, https://cert-agid.gov.it/news/net-walker-il-ransomware-che-ha-beffato-lintera-community/
- Check Point, (2022). The Definitive Guide to Ransom Denial of Service checkpoint.com
- Chen T. M., Jarvis L. (2014). Cyberterrorism: Understanding, assessment, and response. Springer.
- Chen, T. M., & Abu-Nimeh, S. (2011). Lessons from stuxnet. Computer, 44(4), 91-93.
- Cherepanov, A., & Lipovsky, R. (2016). Blackenergy–what we really know about the notorious cyber attacks. Virus Bulletin October.
- Christopher Bronk & Eneken Tikk-Ringas (2013) The Cyber Attack on Saudi Aramco, Survival, 55:2, 81-96, DOI: 10.1080/00396338.2013.784468
- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide. National Institute of Standards and Technology.
- CISA Cybersecurity & Infrastructure Security Agency (2021) CISA Analysis: FY2020 Risk and Vulnerability Assessments

- CISA Cybersecurity & Infrastructure Security Agency (2022) CISA Analysis: FY2021 Risk and Vulnerability Assessments
- CISA Cybersecurity & Infrastructure Security Agency (2023) CISA Analysis: FY2020 Risk and Vulnerability Assessments
- Clarke, R. A., & Knake, R. K. (2010). Cyber War: The Next Threat to National Security and What to Do About It. Harper Collins
- Clusit Community for Security, (2022), SUPPLY CHAIN SECURITY L'importanza di conoscere e gestire i rischi della catena di fornitura, Supply Chain Security
- Coleman, G., (2014). Hacker, hoaxer, whistleblower, spy: The many faces of anonymous. Verso Books.
- Conio G., (2018), Il pensiero critico nell'analisi intelligence, DIS - Dipartimento per le Informazioni e la Sicurezza, Roma
- Conio G., (2020), Intelligence e servizi. Il sistema informativo nazionale. Analytica for intelligence and security studies.
- Crowdstrike, (2020), Intelligence Report CSIT-20081 Technical analysis of the Netwlker ransomware, Crowdstrike global intelligence team.
- CSIRT Italia, (2020), Phishing as a Service Framework, CERT.LV
- CSIRT, (2020), NetWalker Analisi di un ransomware, ACN – Agenzia per la Cybersicurezza Nazionale
- Deng, Y., Lambrecht, A., & Tucker, C. E. (2020). Asymmetric Consequences of Cyber-Vulnerability on Health Services. Available at SSRN 3642485.
- Department of Defense (2019) Dictionary of Military and Associated Terms, s.v. "cyber threat"
- Devanny, J., Martin, C., & Stevens, T. (2021). On the strategic consequences of digital espionage. Journal of Cyber Policy, 6(3), 429-450.
- Ding, J., Qammar, A., Zhang, Z., Karim, A., & Ning, H. (2022). Cyber Threats to Smart Grids: Review, Taxonomy, Potential Solutions, and Future Directions. Energies, 15(18), 6799.
- Ding, S. et al. (2020) "Network Security Defense Model Based on Firewall and Ips," Journal of Intelligent & Fuzzy Systems, 39(6), pp. 8961–8969. doi: 10.3233/JIFS-189294.

- Duncan A. (2020), Cybersecurity in the Covid-19 Era | © 2020 Infosys Consulting
- Durojaye, Henry & Raji, Oluwabukola. (2022). Impact of State and State-Sponsored Actors on the Cyber Environment and the Future of Critical Infrastructure. 10.13140/RG.2.2.36453.06883.
- E. Irmak and İ. Erkek, "An overview of cyber-attack vectors on SCADA systems," 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 2018, pp. 1-5, doi: 10.1109/ISDFS.2018.8355379.
- ENEL, (2021), Risposta alle domande poste prima dell'Assemblea ai sensi dell'art. 127-ter del D. Lgs. n. 58/1998, Assemblea Ordinaria degli Azionisti di Enel S.p.A.
- ENISA - European Union Agency for Cybersecurity, (2016), Strategies for incident response and cyber crisis cooperation
- ENISA - European Union Agency for Cybersecurity, (2017), Overview of cybersecurity and related terminology
- ENISA - European Union Agency for Cybersecurity, (2020), Cyber espionage, ENISA Threat
- ENISA - European Union Agency for Cybersecurity, (2023), Identifying emerging cyber security threats and challenges for 2030
- ENISA (European Union Agency for Cybersecurity), (2021), ENISA THREAT LANDSCAPE FOR SUPPLY CHAIN ATTACKS
- ETDA Electronic Transactions Development Agency, (2022), APT group: Circus Spider
- European Commission. (2017). Report on EU customs enforcement of intellectual property rights: results at the EU border 2016.
- Europol (2021), Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg.
- Falliere, N., Murchu, L. O., & Chien, E. (2011). W32. stuxnet dossier. White paper, symantec corp., security response, 5(6), 29.
- FBI, Federal Bureau of Investigation – Cyber Division, (2020), FBI FLASH Alert number MI-000130-MW Indicators Associated with Netwalker Ransomware
- Federal Bureau of Investigation (FBI). (2020). 2020 Internet Crime Report. FBI.
- FireEye. (2020). Advanced Persistent Threat Groups. FireEye, Inc.

- Forte, D. (2009). Anatomy of a phishing attack: a high-level overview. Network Security, 2009(4), 17-19.
- Gutierrez, C. N., Kim, T., Della Corte, R., Avery, J., Goldwasser, D., Cinque, M., & Bagchi, S. (2018). Learning from the ones that got away: Detecting new forms of phishing attacks. IEEE Transactions on Dependable and Secure Computing, 15(6), 988-1001.
- Hawkins, F. H., & Orlady, H. W. (1993). Human Factors in Flight (2nd ed.). Ashgate.
- Huddleston, J., Ji, P., Bhunia, S., & Cogan, J. (2021, December). How VMware Exploits Contributed to SolarWinds Supply-chain Attack. In 2021 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 760-765). IEEE.
- Hutchins, Eric & Cloppert, Michael & Amin, Rohan. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Leading Issues in Information Warfare & Security Research. 1. International Organization for Standardization. (2018). ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management. Geneva, Switzerland: ISO.
- Jadhav, H., & Madoo, S. THE ETHICS OF CYBER WARFARE: EXPLORING THE USE OF CYBER ATTACK IN MILITARY OPERATIONS.
- Janczewski, L. and Colarik, A. M. (2008) Cyber Warfare and cyber terrorism. Hershey: Information Science Reference.
- Janczewski, Lech & Colarik, A.M.. (2007). Cyber Warfare and Cyber Terrorism. 10.4018/978-1-59140-991-5.
- Jordan, T., Tayler P.A. (2014). Hacktivism and cyberwars: Rebels with a cause? Routledge.
- Jusas, V., Japertas, S., Baksys, T., & Bhandari, S. (2019). Logical filter approach for early stage cyber-attack detection. Comput. Sci. Inf. Syst., 16, 491-514.
- Kao, D., Hsiao, S., & Tso, R. (2019). Analyzing WannaCry Ransomware Considering the Weapons and Exploits. 2019 21st International Conference on Advanced Communication Technology (ICACT), 1098-1107.

- Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2022). Ransomware detection, avoidance, and mitigation scheme: A review and future directions. Sustainability, 14(1), 8. doi:https://doi.org/10.3390/su14010008
- Kizza, J. M. (2013). Ethical and Social Issues in the Information Age. Springer.
- Klimburg A. Tirmaa-Klaar H. 2011. Cybersecurity and Cyberpower: concepts, conditions and capabilities for cooperation for action within the EU. Directorate-General for External Policies, Policy Department.
- Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and Other Botnets. Computer, 50(7), 80–84.
- KPMG (2022), The day after - Recovery, resistance and resilience after an industrial cyber-attack
- Kuersten, Andreas. (2017). The Future of Violence: Robots and Germs, Hackers and Drones—Confronting a New Age of Threat (book review). Terrorism and Political Violence. 29. 1-2. 10.1080/09546553.2017.1341788.
- Kushner, D. (2013). The real story of stuxnet. ieee Spectrum, 50(3), 48-53.
- L. Allodi, T. Chotza, E. Panina and N. Zannone, (2020), "The Need for New Antiphishing Measures Against Spear-Phishing Attacks," in IEEE Security & Privacy, vol. 18, no. 2, pp. 23-34, March-April 2020, doi: 10.1109/MSEC.2019.2940952.
- Landscape 2019- 2020, ISBN: 978-92-9204-354-, DOI: 10.2824/552242
- Langner, R. (2013). Stuxnet and the Future of Cyber War. CreateSpace Independent Publishing Platform.
- Lehman, G., (2016), CYBER ATTACK AGAINST UKRAINIAN POWER PLANTS.
- Lehto, M., and W. Hutchinson. “Mini-Drone Swarms: Their Issues and Potential in Conflict Situations.” Journal of Information Warfare, vol. 20, no. 1, 2021, pp. 33–49. JSTOR, https://www.jstor.org/stable/27036517. Accessed 6 May 2023.
- Lella I. et al. (2022), ENISA Threat Landscape 2022. European Union Agency for Cybersecurity (ENISA), ISBN: 978-92-9204-588-3, DOI: 10.2824/764318
- Lewis, A. J. (2002) Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic & International Studies. Washington DC.

- Liang, G., Weller, S. R., Zhao, J., Luo, F., & Dong, Z. Y. (2016). The 2015 ukraine blackout: Implications for false data injection attacks. IEEE transactions on power systems, 32(4), 3317-3318.
- Litvinov, E. A Undocumented feature or potential vulnerability?
- Malik, S., & Kumar Agrawal, A. Multi-Pronged Approach for Ransomware Analysis. Available at SSRN 4017025.
- Mandrioli, D. (2018). Il caso WannaCry: il fenomeno dei cyber attacks nel contesto della responsabilità internazionale degli Stati. Il caso WannaCry: il fenomeno dei cyber attacks nel contesto della responsabilità internazionale degli Stati, 473-492.
- Marcus Willett (2021) Lessons of the SolarWinds Hack, Survival, 63:2, 7-26, DOI: 10.1080/00396338.2021.190600
- Marelli, M. (2022). The SolarWinds hack: Lessons for international humanitarian organizations. International Review of the Red Cross, 104(919), 1267-1284.
- Matrosov, A., Rodionov, E., Harley, D., & Malcho, J. (2010). Stuxnet under the microscope. ESET LLC (September 2010), 6.
- Mattioli R., Hunter E. N. (2023), Identifying emerging cyber security threats and challenges for 2030 enisa, European Union Agency for Cybersecurity (ENISA), ISBN: 978-92-9204-634-7, DOI: 10.2824/117542
- Mazanec, B. M. (2015) The evolution of cyber war : international norms for emerging-technology weapons. Lincoln: Potomac Books, an imprint of the University of Nebraska Press.
- Mell, P., Bergeron, T., & Henning, D. (2005). Creating a patch and vulnerability management program. NIST Special Publication, 800, 40.
- Mendola C., (2021), Lessons Learned from the SolarWinds Hack: What Went Wrong & How Can Lawyers Help Mitigate the Risk of Cyberattacks
- Miller, J. F. (2013). Supply chain attack framework and attack patterns. MITRE CORP MCLEAN VA.
- Mitnick, K., & Simon, W. (2002). The Art of Deception: Controlling the Human Element of Security. Wiley.
- Morgan S., (2019), 2019 Official Annual Cybercrime Report, Cybersecurity Ventures

- Moses, S., & Rowe, D. C. (2016). Physical security and cybersecurity: Reducing risk by enhancing physical security posture through multi-factor authentication and other techniques. International Journal for Information Security Research (IJISR), 6(2), 667-676.
- N. Kshetri and J. Voas, (2017), Hacking Power Grids: A Current Problem, in Computer, vol. 50, no. 12, pp. 91-95, December, doi: 10.1109/MC.2017.4451203.
- National Audit Office (NAO), (2018), Investigation: WannaCry cyber-attack and the NHS, Department of Health, HC 414 SESSION 2017–2019 25 APRIL 2018
- National Cyber Security Centre (NCSC). (2020). Phishing Attacks. NCSC
- NIST (National Institute of Standards and Technology), (2021), Defending Against Software Supply Chain Attacks, Cybersecurity and Infrastructure Security Agency
- OECD (2007), Development of policies for protection of critical information infrastructures.
- Oest, A., Zhang, P., Wardman, B., Nunes, E., Burgis, J., Zand, A., ... & Ahn, G. J. (2020). Sunrise to sunset: Analyzing the end-to-end life cycle and effectiveness of phishing attacks at scale. In 29th {USENIX} Security Symposium ({USENIX} Security 20).
- PCM DIS, (2019), Cyberbook il glossario di sicurezza cibernetica
- PCM-SISR (Presidenza del Consiglio dei Ministri – Sistema di Informazione per la Sicurezza della Repubblica, (2021), "Relazione sulla Politica dell'Informazione per la Sicurezza 2020"
- PCM-SISR (Presidenza del Consiglio dei Ministri – Sistema di Informazione per la Sicurezza della Repubblica, (2022), "Relazione sulla Politica dell'Informazione per la Sicurezza 2021"
- PCM-SISR (Presidenza del Consiglio dei Ministri – Sistema di Informazione per la Sicurezza della Repubblica, (2023), "Relazione sulla Politica dell'Informazione per la Sicurezza 2022"
- Perez, L. 8 Is Stuxnet the next Skynet? Autonomous cyber capabilities as lethal autonomous weapons systems. Artificial Intelligence and International Conflict in Cyberspace, 186.
- Petropulu, Athina and Diamantaras, Konstantinos I. and Han, Zhu and Niyato, Dusit and Zonouz, Saman, (2019), Contactless Monitoring of Critical Infrastructure [From

the Guest Editors]" in IEEE Signal Processing Magazine, vol. 36, no. 2, pp. 19-21, March 2019, doi: 10.1109/MSP.2018.2890357.
- Polizia di Stato Phishing, (2020), le truffe informatiche legate al Coronavirus
- Polizia di Stato Phishing, (2021), I cybertruffatori sfruttano il nome della Polizia postale
- Polizia di Stato, (2023), I dati 2022 della Polizia postale.
- Radware (2019), A Guide To State-Sponsored Cyberthreats. Who Are the Adversaries and How to Defend Against Them
- Rafiullah Khan, Peter Maynard and Kieran McLaughlin et al., (2016), Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid. DOI: 10.14236/ewic/ICS2016.7
- Raponi, S., Caprolu, M., & Di Pietro, R. (2021). Beyond SolarWinds: The Systemic Risks of Critical Infrastructures, State of Play, Future Directions. ITASEC, 21, 07-09.
- Reuters T. (2014), Thoughts on Cyber Security – Liability, Damages & insurance, su Fintech Law Mar/Apr 2014, Vol1, Issue 2,
- SANS Institute. (2016). Securing Industrial Control Systems-2016. SANS Institute.
- Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge: Cambridge University Press. doi:10.1017/9781316822524
- Setola R., Theocharidou M. 2016. “Managing the Complexity of Critical Infrastructures. A Modelling and Simulation Approach in Studies in Systems”. Decision and Control Vol. 90: Chapter 2 Modelling Dependencies Between Critical Infrastructures. Springer Open.
- Shehod, A. (2016). Ukraine power grid cyberattack and US susceptibility: Cybersecurity implications of smart grid advancements in the US. Cybersecurity Interdisciplinary Systems Laboratory, MIT, 22, 2016-22.
- Singer, P. W. and Friedman, A. (2014) Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press (What everyone needs to know).
- SMD (Stato Maggiore Difesa), (2021), Concetto Scenari Futuri: tendenze e implicazioni per la Sicurezza e la Difesa. Stato Maggiore Difesa.

- SMD (Stato Maggiore Difesa), (2022), Approccio della Difesa alle Operazioni Multidominio.
- Smith, J. (2020). Cybersecurity Threats and Vulnerabilities. In Handbook of Research on Cyber Crime and Information Privacy (pp. 1-20). IGI Global.
- Steingartner, W., & Galinec, D. (2021). Cyber threats and cyber deception in hybrid warfare. Acta Polytechnica Hungarica, 18(3), 25-45
- Steingartner, William & Galinec, Darko & Kozina Assistant Professor, Andrija. (2021). Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model. Symmetry. 13. 597. 10.3390/sym13040597.
- Sterle, L., & Bhunia, S. (2021, October). On solarwinds orion platform security breach. In 2021 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/IOP/SCI) (pp. 636-641). IEEE.
- Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security. NIST Special Publication 800-82 Revision 2. National Institute of Standards and Technology.
- Strucl D. (2021). Comparative study on the cyber defence of NATO Member States. NATO CCDCOE.
- Sullivan, J. E., & Kamensky, D. (2017). How cyber-attacks in Ukraine show the vulnerability of the US power grid. The Electricity Journal, 30(3), 30-35.
- Swascan, (2023), Threatland Report cyber security Q1: Dal Ransomware Al phishing, tutti i trend del 2023.
- Symantec. (2019). Internet Security Threat Report. Symantec Corporation
- Tang, Yi and Qian Chen and Mengya Li and Wang, Qi and Ni, Ming and XiangYun Fu, (2016). Challenge and evolution of cyber attacks in Cyber Physical Power System, IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC), Xi'an, China, 2016, pp. 857-862, doi: 10.1109/APPEEC.2016.7779616.
- Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L., ... & Bursztein, E. (2017, October). Data breaches, phishing, or malware? Understanding the risks of stolen credentials. In Proceedings of the 2017 ACM SIGSAC conference on computer and communications security (pp. 1421-1434).

- Trautman, L. J., & Ormerod, P. C. (2018). Wannacry, ransomware, and the emerging threat to corporations. Tenn. L. Rev., 86, 503.
- U.S. Air Force, (2021), Air Force Doctrine Publication 3-60, Targeting
- U.S. Air Force, (2023), Air Force Doctrine Publication 3-12, Cyberspace Operations.
- U.S. Department of Defense. Joint Publication 3-13 Information Operations, February 2006. URL http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.
- U.S. Department of Defense. Joint Publication 3-60 Joint Targeting, April 2007. URL http://www.dtic.mil/doctrine/new_pubs/jp3_60.pdf.
- Verizon. (2022). Data Breach Investigations Report DBIR 2008-2022
- Wallis, T., Johnston, C., & Khamis, M. (2021). Interorganizational cooperation in supply chain cybersecurity: A cross-industry study of the effectiveness of the UK implementation of the NIS Directive. Information and Security: An International Journal, 48, 36-68.
- Whitman, M. E., & Mattord, H. J. (2016). Principles of information security. Cengage Learning.
- Whitman, M. E., & Mattord, H. J. (2017). Principles of Incident Response and Disaster Recovery. Cengage Learning.
- Wittes, B., & Blum, G. (2015). The Future of Violence: Robots and Germs, Hackers and Drones - Confronting A New Age of Threat. Basic Books.
- Yurtayeva, k, (2022), Cyberaggression as a part of hybrid war against ukraine. In кібербезпека в україні: правові та організаційні питання international scientific-practical conference" Cybersecurity in Ukraine: Legal and (p. 8).
- Zheng, T., Liu, M., Puthal, D., Yi, P., Wu, Y., & He, X. (2022). Smart Grid: Cyber Attacks, Critical Defense Approaches, and Digital Twin. arXiv preprint arXiv:2205.11783.

SITI WEB

- (Direttiva NIS) DIRETTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L1148
- (Direttiva NIS2) DIRETTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022L2555
- 15 Stealthy Cyberthreats You Need To Watch Out For https://www.forbes.com/sites/forbestechcouncil/2020/08/25/15-stealthy-cyber-threats-you-need-to-watch-out-for/
- Agenzia per la Cybersicurezza Nazionale (ACN) https://www.acn.gov.it/
- Cibersicurezza delle reti e dei sistemi informatici (2022) https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=LEGISSUM:4637829
- CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence), (2017), WannaCry Campaign: Potential State Involvement Could Have Serious Consequences, https://ccdcoe.org/news/2017/wannacry-campaign-potential-state-involvement-could-have-serious-consequences/
- Cisco, (2018), What Is Malware? Cisco Systems, Inc. https://www.cisco.com/site/us/en/products/security/what-is-malware.html
- Cisco, (2023), What Is Identity Access Management (IAM)?, https://www.cisco.com/c/en/us/products/security/identity-services-engine/what-is-identity-access-management.html
- Critical Infrastructure su https://www.dhs.gov/science-and-technology/critical-infrastructure
- Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride! https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030
- Di Giuseppe C. (2022) Il ransomware Wannacry https://www.analisidifesa.it/2022/05/il-ransomware-wannacry/

- DIS – Dipartimento per le informazioni e la Sicurezza (2019) Glossario https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/06/glossario-intelligence-2019.pdf
- ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021?v2=1
- F3RM1 Foundation (2022), Intelligenza Artificiale: le sfide per la sicurezza https://f3rm1.cloud/articoli/intelligenza-artificiale--le-sfide-per-la-sicurezza
- F3RM1 Foundation (2022), Smart Working e Sicurezza Informatica: quali sono i potenziali rischi e le possibili soluzioni? https://f3rm1.cloud/articoli/smart-working-e-sicurezza-informatica--quali-sono-i-potenziali-rischi-e-le-possibili-soluzioni--1
- F3RM1 Foundation (2023), ChatGTP e l'evoluzione dell'intelligenza artificiale che impatti per la cyber sicurezza? https://f3rm1.cloud/articoli/chatgtp-e-l---evoluzione-dell---intelligenza-artificiale-che-impatti-per-la-cyber-sicurezza--1
- Fernandez A. (2022) Regulating Deep Fakes in the Proposed AI Act https://www.medialaws.eu/regulating-deep-fakes-in-the-proposed-ai-act/
- L'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) su OECD.org
- RAND Topics: Cyber Warfare https://www.rand.org/topics/cyber-warfare.html
- Regulating Deep Fakes in the Proposed AI Act https://www.medialaws.eu/regulating-deep-fakes-in-the-proposed-ai-act/
- Ferla D. (2020), WannaCry Dissected, an in-depth analysis of the malware outbreak, Università di Bologna, http://www.lia.deis.unibo.it/Courses/SicurezzaM1920/lab/lab00_wannacry.pdf

CONVEGNI/CORSI

- Video intervento di Giovanni Gagliano (Stato Maggiore della Difesa) a "Cyber-Sec2023 - Nuovi Domìni, Guerre Ibride e Cooperazione")
- Video intervento di Nunzia Ciardi (Vice Direttore Generale, ACN) a "Cyber-Sec2023 - Nuovi Domìni, Guerre Ibride e Cooperazione"
- SIOI Roma - Master in Protezione Strategica del Sistema Paese: Cyber Intelligence, Big Data e Sicurezza delle Infrastrutture Critiche, edizione 2020-2021

Pubblicato nel giugno 2024
Società Italiana di Intelligence
SOCINT Press
https://press.socint.org

979-12-80111-55-5